

CHOICE, unlimited

Creating and Enhancing Opportunities Within Local Communities

General HIPAA Compliance Policy and Confidentiality of Individual Record Set

I. Policy:

All employees must be familiar with and comply with the federal HIPAA privacy regulations. The HIPAA privacy regulations impose a uniform, national policy on the confidentiality of service recipient records and impose penalties for failure to comply. These federal standards are in addition to any existing state or local privacy standards that may already be in place. The HIPAA regulations are enforced by the Secretary of Health and Human Services (HHS) Center for Medicare and Medicaid Services (CMS) Office of Civil Rights beginning on April 14, 2003.

II. Glossary of Terms

Confidential Data: Highly sensitive information about an individual and is given the highest level of protection. It cannot be shown to the public or to the individual who the information is about. (e.g. names of persons reporting maltreatment of a vulnerable adult or child)

HIPAA: Health Insurance Portability and Accountability Act, a federal act of 1996.

HIPAA Privacy Officer: Individual who ensures policy and practices are within the standards

Individual: Means a person who receives services from CHOICE, unlimited.

Individual Record Set: Means the information CHOICE, unlimited maintains or keeps on an individual and that the individual is entitled to see. Information included in the Individual Record Set includes:

- Assessments
- Progress notes / Data sheets
- Summaries
- Medication Administration records
- Treatment records from other providers
- Intake information
- Discharge information
- Billing and payment records
- Case Management records (CSSP)
- CSSPA / Individual Abuse Prevention Plans (IAPP)
- Outcomes data and summaries
- Outcome plans
- Job search / Job development records
- Any other records used to make decisions about the person
- Records from which a particular individual can be identified

Information that is not considered part of the Individual Record Set includes:

- Informal staff documentation
- Psychotherapy notes prepared by a psychotherapist
- Internal investigation information
- Employee personnel records and information
- Information compiled in reasonable anticipation of a civil, criminal or administration action or proceeding.

Individually Identifiable Health Information: Any information, including demographic information collected from an individual, that (A) is created or received by a health care provider, health plan,

employer, or health care clearinghouse; and (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual, and:

- Identifies the individual; or
- With respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

Private Data: Information that can be seen by the individual who the information is about but not by the public.

Private Health Information (PHI): Private health information as defined under HIPAA regulations. Any information, in any form or medium, which has been created or received by:

- Providers of health care
- Health care plans (insurances)
- Health care “clearinghouses,” which are organizations that provide information management or other services to health care providers or health care plans.

AND

- Relates to at least one of the following: Past, present or future-
 - Physical or mental health of an individual
 - The provision of health care to an individual
 - An individual’s eligibility for health care
 - Payment for the provision of health care to an individual
 - An individual’s past treatment, payment, or eligibility
 - Includes all health-related information about the physical or mental health of an individual.

Protected Information: Includes information that is private, confidential and/or private health information (PHI); data that identifies, or could identify, the person who the information is about.

Summary Data: Statistical data and reports derived from data on individuals but in which individuals are not identified and from which neither their identities nor any other characteristic that could uniquely identify an individual is ascertainable.

III. Procedure for Confidentiality of Information

Information concerning individuals served by CHOICE, unlimited is protected. This means that information about specific people who receive services may not be released to anyone unless:

- a. The individual or the individual’s legal representative has signed a valid, current Release of Information form; or
- b. You have received a court order for the information; or
- c. The release of information is otherwise authorized by law.

Procedure: Forward all requests for individual service recipient information to the Executive Director for approval. Do not release information without approval for the release from the Executive Director, or if the Executive Director cannot be reached contact a Program Director.

If there is a question about whether the requested information can be released, do not release any information until the Executive Director (HIPAA Privacy Officer) approves the release.

Failure to Follow Confidentiality Policy: Employees who release private information improperly or who fail to follow this procedure will face disciplinary action.

Releasing Information with a Release Form: Private data may be used by and disseminated to any person or agency if the individual, who is the subject of the data, have given their informed consent. The informed consent (valid authorization under HIPAA) must include specific core elements:

- The information to be used or disclosed;
- The names of the person(s) authorized to use, disclose and receive the information;
- The purpose of the use or disclosure;
- An expiration date or event, not to exceed one year beyond the date the consent was obtained
- The dated signature of the individual;
- And statements concerning the right to revoke the authorization in writing;
- The ability or inability to set conditions of treatment, payment, or eligibility for benefits on the authorization;
- And the potential for re-disclosure by the recipient.

The authorization must be written in plain English, and a copy must be provided to the individual. The individual may revoke the authorization at any time in writing, with limited exceptions.

Releasing Information without a Release Form:

HIPAA allows certain “social responsibility” disclosures to be made without a release from the individual. Generally, these include the following:

- Disclosure necessary to report abuse or neglect of child or vulnerable adult;
- Disclosure for some, but not all law enforcement purposes, including grand jury proceedings;
- Administrative or judicial proceedings in certain situations;
- Certain public health information disclosures;
- Health oversight activities such as licensing or certification inspections;
- In response to a court order; or in response to a subpoena, but only if:
 - The party seeking the information assures CHOICE, unlimited that reasonable efforts have been made to get a protective order from the court preventing further disclosure of the information; or
 - The party who is the subject of the information has been given notice of the request, and the time to object has passed.
 - CHOICE, unlimited has attempted to notify the individual to either obtain consent or give the individual the opportunity to object to the disclosure.
- Certain disclosures about people who have died;
- Certain research activities;
- To avert a serious threat to health or safety;
 - An individual is injured or becomes suddenly ill and needs immediate medical attention.
 - An outbreak of a highly contagious disease has occurred.
 - An individual makes a serious threat to harm another specific person.
 - There is a risk to the health or safety of the individual or other persons.
- Note: In situations in which you would normally need to get a signed release, as soon as possible after the emergency situation ends, you must:
 - Document the release of all protected information, to whom it was released and the purpose within the individual’s file.
 - Try to obtain a signed release from the individual.
 - Provide a privacy notice (Tennessee Warning) to the individual.
- For specialized government functions;
- Disclosures relating to organ donations;
- Workers’ Compensation disclosures

If you are unsure about whether the information can be released without a release, consult the Executive Director, or in their absence, a Program Director.

IV. Procedure for ongoing Privacy and Security Assessment

Staff monitors and assesses access to individual information on an ongoing basis. This includes:

- a. Paper Records: All paper individual records are created, maintained and stored in a physical location where other service recipients, unauthorized staff or visitors may not have access to them. This includes paper records in files, at fax machines, and in printers and copiers.
- b. Electronic Records: All individual electronic records are created, maintained and stored in a way that other service recipient, unauthorized staff, visitors or outsiders may not have access to them. This includes access to computers at the office, at employee's homes, and on laptop computers. It may involve the use of passwords, automatic closure of files or encryption.
- c. Verbal Communications: All verbal communication about individuals is conducted in a way that other service recipients, unauthorized staff, visitors or others do not overhear.
- d. Understanding and Monitoring Changes in State Privacy Laws: State privacy laws may impose greater or lesser protections to individual health information. If the state and federal requirements conflict, CHOICE, unlimited will follow the law that provides the greater protection to the individual's privacy. If there is a question about which law governs, the request will be referred to the Executive Director and no information will be disclosed until the matter is decided.

Procedure: Protected information must be safeguarded from unlawful disclosure regardless of the form the information is in. Staff monitors and assesses access to individual information on an ongoing basis. This includes:

- Paper Records: All information concerning an individual must be kept in a file separate from any other individual. All individual files must be kept in a supervised or locked area to prevent unauthorized individuals from accessing the information. When sending a fax containing protected information, call the individual receiving the fax prior to sending to ensure they are able to pick up the fax in a timely manner. Remove any printed material containing protected information from printers and copiers in a timely manner.
- Electronic Records: Staff will not share their computer passwords. When leaving a computer workstation, staff will turn on their screen saver, lock their work station or log off the network. Individual information is not shared by e-mail unless the individual has signed a consent authorizing the use of e-mail for this purpose. Secure and encrypted email processes will be used when transmitting confidential information.
- Conversations identifying individuals will be conducted in a private area. If this is not possible, conversations should be held in a lowered voice volume so others cannot overhear the conversation. This includes face to face and telephone conversations.

V. Procedure for Disclosure

Minimum Necessary:

CHOICE, unlimited is charged with assuring the privacy of the individuals it serves. The law requires that staff view, use, and release only the protected information that is necessary to do your job.

Procedure: Anytime information from the Individual Record Set is released, CHOICE, unlimited staff must release only the minimum necessary information required to respond to the disclosure request.

Good practices that comply with the Minimum Necessary Rule include:

- Discuss an individual's case ONLY as needed to do your job.

- Whenever possible, limit review of an individual's records to information required to do your job.
- Do not look up information about family members, friends, neighbors, or anyone else who is not assigned to you.
- Where the law permits release of protected information without a release form, try to limit the information to what is necessary to get the job done.

CHOICE, unlimited will conduct a review of all instances of use or disclosure of private health information in violation of policies and procedures brought to their attention. The Privacy Officer will be notified of any such instance. CHOICE, unlimited will mitigate, to the extent possible, any harmful effect that is known from such use of disclosure of private health information.

Verification:

CHOICE, unlimited will verify the identity of a person requesting individual information to make sure that:

- a. the person has the authority to receive the information, and
- b. that the person who is requesting the records is the same person who is authorized to receive them.

Procedure:

Before releasing any individual information, staff must:

- a. request a copy of the authorization (such as a release, court document or other information appointing the person as a legal representative)
- b. ask for appropriate identification such as a driver's license, state issued identification card, government issued badge or government letterhead,
- c. copy the verification information and put it in the individual's file.

Disclosures to Business Associates Policy

Certain people and businesses may require access to portions of the individual record set to do their work. CHOICE must have a HIPAA Business Associate Agreement with these businesses before any information can be released to them. (See Business Associate Agreement form.)

Procedure: Maintain a signed copy of the agreement on a permanent basis.

Summary Data:

Summary data, as defined by Minnesota law, may be released to the public without consent of the subject individuals.

Procedure: All summary data will be approved by the Privacy Officer prior to release to ensure compliance with Minnesota law.

VI. Procedure for Individual's Access to the Individual Record Set

Response to a Request to Inspect and Copy the Individual Record Set:

Individuals have the right to inspect and copy information in their Individual Record Set. Individuals must make their request in writing. Generally, the individual is permitted to inspect and copy their record unless there is medical or program reason, as determined by a licensed professional, to deny

access to all or part of the Individual Record Set. The individual may request a review of the decision by a second person within CHOICE, unlimited.

CHOICE, unlimited will retain a copy of the written request in the individual's file. CHOICE, unlimited may charge a reasonable fee for copying records.

CHOICE, unlimited will respond to a request to inspect and copy records within 30 days, or within 60 days if an extension is requested.

Response to Request an Amendment to the Individual Record Set:

When CHOICE, unlimited receives a request from an individual to amend information from the individual record, CHOICE, unlimited will acknowledge receipt of the request immediately by sending a Letter to Acknowledge Request for Amendment of Individual Record Set. (See form; explanation included on the form)

CHOICE, unlimited will provide a substantive response to an individual's request to amend the Individual Record Set within 30 days. CHOICE, unlimited will:

- Amend the Individual Record Set, and send the Letter Granting Request for Amendment or
- Deny the request and provide a written explanation of why CHOICE, unlimited will not amend the Individual Record Set and send the Letter Denying Request for Amendment; or
- Request one 30-day extension if it is not possible to comply in 30 days.

CHOICE, unlimited may deny access to an Individual's Record Set if the access request may endanger the life or physical safety of the individual or another person.

Response to Request for Accounting for Disclosures:

CHOICE, unlimited documents disclosure of individual information and makes an accounting of these disclosures available to the individual upon request. The accounting must cover the last six years, beginning with disclosure made after April 13, 2003.

CHOICE, unlimited will keep a record of accountings requested and received in the individual file.

CHOICE, unlimited does not provide accountings for disclosures to:

- Carry out treatment, payment or health care operations
- Disclosures to the individual, or
- Disclosures for national security or intelligence purposes.

Requests for Alternative Communication:

Individuals may request that CHOICE, unlimited communicate with them in an alternative way or at an alternative location. For example, an individual may ask that all communication be written rather than verbal, or that communication be sent to work rather than home.

CHOICE, unlimited will document these requests, and will accommodate all reasonable requests for alternative communications.

Requests for Restricted use of Individual Information:

Individuals may request that CHOICE, unlimited restrict use and disclosure of the individuals' records for ordinary treatment, payment or healthcare operations. For example, the individual may ask that a particular employee, such as a CHOICE, unlimited employee who is a relative, not be allowed access to individual information. Requests will be made in writing to the Executive Director. CHOICE, unlimited will either grant or deny such a request, and document the request and the response in the individual's record.

If CHOICE, unlimited grants the request to Restrict Use of the individual information, staff must abide by it except in the case of a medical emergency. An individual may not request restrictions on disclosure to themselves, or for which a release is not required.

VII. Privacy Notices

CHOICE, unlimited has a Notice of Privacy Practices that describes its procedures on the use and release of Individual Information. This notice may be amended from time to time.

CHOICE, unlimited will disseminate the privacy notice and any amended notices to all individuals receiving services. This notice will be disseminated as required by HIPAA federal regulations, upon future changes in CHOICE, unlimited privacy policies and upon initiation of services from CHOICE, unlimited. CHOICE unlimited will keep proof of distribution of the notice in the individual's file. Individuals will sign and return consents to use of their information and an acknowledgement of the terms of the Notice of Privacy Practices. The signed notice is kept in the individual's plan file.

VIII. Staff Training

New Employee Orientation:

CHOICE, unlimited trains all new employees regarding privacy practices, including HIPAA privacy standards as part of their orientation procedure. This training is documented in the employee's training file.

Ongoing Training:

CHOICE, unlimited trains all employees on Privacy Practices, including HIPAA privacy standards, on a regular basis. This training is documented in the employee's training file.

Privacy Officer

Kristie Buchman is CHOICE, unlimited's HIPAA Privacy Officer. She has the responsibility to answer questions about HIPAA privacy compliance issues and to handle employee or service recipient concerns or complaints about the organizations individual record policies. The Privacy Officer can be reached by:

Phone: (218) 724-5869

E-mail: kbuchman@choiceunlimited.org

Mail: 1829 East Superior Street, Duluth, MN 55812

Fax: (218) 724-0359

IX. Procedures for Complaint and Anti-Retaliation

Complaints Procedure:

Individuals and employees may make complaints to CHOICE, unlimited about its HIPAA policies, compliance with its policies or procedures, and compliance with the HIPAA privacy regulations. CHOICE, unlimited will not retaliate against an individual or employee who makes a complaint, participates in a HIPAA investigation, or who opposes any unlawful act relating to the privacy regulations. CHOICE, unlimited's Privacy Officer will maintain a record of all complaints and resolutions. The complaints will be reviewed by the Board of Directors as needed on an annual basis.

Complaints may be made in person, by phone, by email, or in writing by contacting:

Kristie Buchman

Phone: (218) 724-5869

E-mail: kbuchman@choiceunlimited.org

Mail: 1829 East Superior Street, Duluth, MN 55812

Fax: (218) 724-0359

In addition, individuals or employees may file complaints with the:

Privacy Official:

Minnesota Department of Human Services

P.O Box 64998

St. Paul, MN 55164-0998

Office of Civil Rights

Medical Privacy, Complaint Division

U.S. Department of Health and Human Services

200 Independence Avenue, SW, HHH Building, Room 509H

Washington, D.C. 20201

Phone: 866-627-7748

TTY: 866-788-4989

If you need legal assistance contact the Minnesota Disability Law Center at 218-722-5625

2.I.10 General HIPAA Compliance Policy & Confidentiality of Individual Record Set

Reviewed and Revised 8/18/2022

Policy Manual 2, Intake packet, Employee Handbook