Data Privacy

DEPARTMENT: 245D	**POLICY NO:** 245D-004
AFFECTED STATES: MN	**OWNER:** ANGIE OUJIRI

PURPOSE

The purpose of this policy is to establish guidelines that promote service recipient rights ensuring data privacy and record confidentiality of persons served.

POLICY

According to MN Statutes, section 245D.04, subdivision 3, persons served by the program have protection-related rights that include the rights to:

- Have personal, financial, service, health, and medical information kept private, and be advised of disclosure of this information by the company.
- Access records and recorded information about the person in accordance with applicable state and federal law, regulation, or rule.

Orientation to the person served and/or legal representative will be completed at service initiation and as needed thereafter. This orientation will include an explanation of this policy and their rights regarding data privacy. Upon explanation, the Designated Manager and/or Designated Coordinator will document that this notification occurred and that a copy of this policy was provided.

This company encourages data privacy in all areas of practice and will implement measures to ensure that data privacy is upheld according to MN Government Data Practices Act, section 13.46. The company will also follow guidelines for data privacy as set forth in the Health Insurance Portability and Accountability Act (HIPAA) to the extent the company performs a function or activity involving the use of protected health information and HIPAA's implementing regulations, Code of Federal Regulations, title 45, parts 160-164, and all applicable requirements. The CEO will exercise the responsibility and duties of the "responsible authority" for all program data, as defined in the Minnesota Data Practices, MN Statutes, chapter 13. Data privacy will hold to the standard of "minimum necessary" which entails limiting protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

PROCEDURE

Access to Records and Recorded Information and Authorizations

1. The person served and/or legal representative have full access to their records and recorded information that is maintained, collected, stored, or disseminated by the company. Private data are records or recorded information that includes personal, financial, service, health, and medical information.
2. Access to private data in written or oral format is limited to authorized persons. The following company personnel may have immediate access to persons' private data only for the relevant and necessary purposes to carry out their duties as directed by the Support Plan and/or Support Plan Addendum:
    a. Executive staff.
    b. Administrative staff.
    c. Financial staff.
    d. Nursing staff including assigned or consulting nurses.
    e. Management staff including the Designated Coordinator and/or Designated Manager.
    f. Direct support staff.
3. The following entities also have access to persons' private data as authorized by applicable state or federal laws, regulations, or rules:
    a. Case manager.
    b. Child or adult foster care licensor, when services are also licensed as child or adult foster care.
    c. Minnesota Department of Human Services and/or Minnesota Department of Health.
    d. County of Financial Responsibility or the County of Residence's Social Services.
    e. The Ombudsman for Mental Health or Developmental Disabilities.
    f. US Department of Health and Human Services.
    g. Social Security Administration.
    h. State departments including Department of Employment and Economic Development (DEED), Department of Education, and Department of Revenue.

i. County, state, or federal auditors.
j. Adult or Child Protection units and investigators.
k. Law enforcement personnel or attorneys related to an investigation.
l. Various county or state agencies related to funding, support, or protection of the person.
m. Other entities or individuals authorized by law.

4. The company will obtain authorization to release information of persons served when consultants, sub-contractors, or volunteers are working with the company to the extent necessary to carry out the necessary duties.
5. Other entities or individuals not previously listed who have obtained written authorization from the person served and/or legal representative have access to written and oral information as detailed within that authorization. This includes other licensed caregivers or health care providers as directed by the release of information.
6. Information will be disclosed to appropriate parties in connection with an emergency if knowledge of the information is necessary to protect the health or safety of the person served or other individuals or persons. The Designated Coordinator and/or Designated Manager will ensure the documentation of the following:
    a. The nature of the emergency.
    b. The type of information disclosed.
    c. To whom the information was disclosed.
    d. How the information was used to respond to the emergency.
    e. When and how the person served and/or legal representative was informed of the disclosed information.
7. All authorizations or written releases of information will be maintained in the person's service recipient record. In addition, all requests made to review data, have copies, or make alterations, as stated below, will be recorded in the person's record including:
    a. Date and time of the activity.
    b. Who accessed or reviewed the records.
    c. If any copies were requested and provided.

Request for Records or Recorded Information to Be Altered or Copies

1. The person served and/or legal representative has the right to request that their records or recorded information and documentation be altered and/or to request copies.
2. If the person served and/or legal representative objects to the accuracy of any information, staff will ask that they put their objections in writing with an explanation as to why the information is incorrect or incomplete.
    a. The Designated Coordinator and/or Designated Manager will submit the written objections to the CEO who will make a decision in regard to any possible changes.
    b. A copy of the written objection will be retained in the person's service recipient record.
    c. If the objection is determined to be valid and approval for correction is obtained, the Designated Coordinator and/or Designated Manager will correct the information and notify the person served and/or legal representative and provide a copy of the correction.
    d. If no changes are made and distribution of the disputed information is required, the Designated Coordinator and/or Designated Manager will ensure that the objection accompanies the information as distributed, either orally or in writing.
3. If the person served and/or legal representative disagrees with the resolution of the issue, they will be encouraged to follow the procedures outlined in the Policy and Procedure on Grievances.

Security of information

1. A record of current services provided to each person served will be maintained on the premises of where the services are provided or coordinated. Records will be maintained at the company's program office. Files will not be removed from the program site without valid reasons and security of those files will be maintained at all times.

2. The Designated Coordinator and/or Designated Manager will ensure that all information for persons served are secure and protected from loss, tampering, or unauthorized disclosures. This includes information stored by computer for which a unique password and user identification is required.

3. No person served and/or legal representative, staff, or anyone else may permanently remove or destroy any portion of the person's record.
4. The company and its staff will not disclose personally identifiable information about any other person when making a report to each person and case manager unless the company has the consent of the person. This also includes the use of other person's information in another person's record.
5. Written and verbal exchanges of information regarding persons served are considered to be private and will be done in a manner that preserves confidentiality, protects their data privacy, and respects their dignity.
6. All staff will receive training at orientation and annually thereafter on this policy and their responsibilities related to complying with data privacy practices.