



<b>Policy Name:</b>	<b>Data Privacy</b>
<b>Policy Code:</b>	<b>406</b>
<b>Policy Purpose:</b>	To protect private data. Rise recognizes the right of each person receiving services to confidentiality and data privacy. This policy applies to all team members, temporary staff, volunteers, and person or agencies under contract with Rise (paid or unpaid).

## I. Overview

This policy provides general guidelines and principles for safeguarding service recipient rights to data privacy as stated in Minnesota Government Data Practices Act and the HIPAA and HITECH acts, which seek to protect the privacy of the individuals about whom government agencies, their subdivisions, and agencies under contract with them collect data. It also facilitates the release of information, which is public.

- A. This policy is also in compliance with section 245D.04, subdivision 3(a) and access to their records under section 245D.095, subdivision 4, of the 245D Home and Community-based Services Standards.

## II. Procedures

### A. Private Data

1. Private data includes all information on individuals that has been gathered by Rise or from other sources for program purposes as contained in an individual case file or secure electronic file, including their presence and status in this program.
2. Data is private if it is about individuals and is classified as private by state or federal law. The following persons are permitted access to private data:
  - a. The individual who is the subject of the data or a legal representative.
  - b. Anyone to whom the individual gives signed consent to view the data.
  - c. Employees of the welfare system whose work assignments reasonably require access to the data. This includes team members in this program.
  - d. Anyone the law says can view the data.

- e. Data collected within the welfare system about individuals is considered welfare data. Welfare data is private data on individuals; including medical and/or health data. Agencies in the welfare system include, but are not limited to:
    - U.S. Departments of Health and Human Services, Labor, Agriculture, and the Social Security Administration.
    - Minnesota Departments of Human Services, Employment and Economic Development (DEED), Labor and Industry, Revenue, Veterans Affairs, Education, Corrections, and Human Rights.
    - The Ombudsman for Mental Health or Developmental Disabilities.
    - Local social services agencies, including a person's case manager.
    - Human services boards.
    - Adult or Child Protection units and investigators.
    - To a court via a valid court order.
    - To appropriate parties in an emergency.
    - Other entities or individuals authorized by law.
    - Persons, agencies, institution, organization and other entities under contract to one of the above agencies, only to the extent of the contract.
    - Attorney General, county attorney or other law enforcement officials, if necessary for program purposes.
  - f. Once informed consent has been obtained from the person or the legal representative there is no prohibition against sharing welfare data with other persons or entities within the welfare system for the purposes of planning, developing, coordinating and implementing needed services.
3. Data created prior to the death of a person retains the same legal classification (public, private, confidential) after the person's death that it had before the death.

## **B. Security of Information**

1. The Program Manager will ensure that all information for persons served is 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.
2. No person served and/or legal representative, team member, or anyone else may permanently remove or destroy any portion of the person's record.
3. 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.
4. All team members will receive training at orientation and annually thereafter on this policy and their responsibilities related to complying with data privacy practices.

5. Program files for persons served may be destroyed seven years after discharge.

### **C. Providing Notice**

1. At the time of service initiation, the person and his/her legal representative, if any, will be notified of this program's data privacy policy. Team members will document that this information was provided and explained to the individual and/or their legal representative in the individual case file.

### **D. Obtaining Informed Consent or Authorization for Release of Information**

1. At the time informed consent is being obtained team members must tell the person or the legal representative individual the following:
  - a. Why the data is being collected.
  - b. The purpose and how Rise intends to use the information.
  - c. The purposes of the information we collect are listed below. Depending upon the program, the data may be used for the following purposes:
    - Determining eligibility for services provided by this agency.
    - Providing effective care and treatment of medical/social/psychological problems.
    - Enabling Rise to collect federal, state or county funds for aids and services.
    - Enabling Rise to meet accreditation standards.
    - Preparing statistical reports and evaluations.
    - Investigating facility complaints or reports of abuse, fraud, or misconduct.
    - Conducting program and financial audits.
    - Collecting reimbursement from other agencies or individuals or liable third parties, including health insurance carriers for the services or assistance Rise provides.
    - Determining whether protective services are needed.
    - Research.
    - Determining service plans.
    - Informing team members of progress.
  - d. Whether the individual may refuse or is legally required to furnish the information:
    - In most cases, persons served are not legally required to provide the information requested. If legally required to supply the information requested, they will be informed of the law which requires it.
    - If an individual does not provide the information requested, Rise may not be able to determine eligibility for services. As a result, Rise may not be able to serve the person without the requested information.

- e. How the individual can see and get copies of the data collected about them; and any other rights that the individual may have regarding the specific type of information collected.
  - f. Rise's Notice of Privacy Practices regarding protected health information, and how to respond if any breach of protected health information occurs.
  - g. The identity of other persons or agencies authorized by statute to receive the information.
2. A proper informed consent or authorization for release of information form must include these factors (unless otherwise prescribed by the HIPAA Standards of Privacy of Individually Identifiable Health Information 45 C.F.R. section 164):
- a. Be written in plain language.
  - b. Be dated.
  - c. Designate the particular agencies or person(s) who will get the information.
  - d. Specify the information which will be released.
  - e. Indicate the specific agencies or person who will release the information.
  - f. Specify the purposes for which the information will be used immediately and in the future.
  - g. Contain a reasonable expiration date of no more than one year.
  - h. Specify the reasons and consequences for the person by signing the consent form, including the following information:
    - That State and federal privacy laws protect records.
    - The reason they are being asked to release this information.
    - That they do not have to consent to the release of this information. But not doing so may affect this program's ability to provide needed services.
    - That if they do not consent, the information will not be released unless the law otherwise allows it.
    - Consent may be withdrawn with a written notice at any time, but this written notice will not affect information this program has already released.
    - The person(s) or agency(ies) who receive the information may be able to pass it on to others.

- If information is passed on to others by this program, it may no longer be protected by this authorization.
  - The consent will end one year from the date it is signed unless the law allows for a longer period.
- i. All informed consent documents will be maintained in the person's individual case file or secure electronic file.

#### **E. Team Member Access to Private Data**

1. Team members do not automatically have access to private data about the persons served by this program or about other team members or agency personnel.
2. Team members must have a specific work function need for the information. Private data about persons are available only to those program employees whose work assignments reasonably require access to the data; or who are authorized by law to have access to the data.
3. Any written or verbal exchanges about a person's private information by team members with other team members or any other persons will be done in such a way as to preserve confidentiality, protect data privacy, and respect the dignity of the person whose private data is being shared.
4. As a general rule, doubts about the correctness of sharing information should be referred to the supervisor.

#### **F. Violations of this Policy**

Looking up or talking about a persons served health or private information without a permitted reason, as described above, is not allowed. This includes information contained in both paper files and records in NetSmart. Generally, access, use or disclosure of protected health information in a way that is not described in this policy is not permitted. Even if the team member has a permitted reason, the use, access or disclosure must follow the proper procedures.

Examples of conduct that violate this policy include, but are not limited to, the following:

1. Inadvertently mailing, emailing, or faxing private information to the wrong person.
2. Bringing a file containing private information home to complete work without permission.
3. Viewing or Printing information from NetSmart regarding persons served that you do not work with.

4. Bringing a file containing private information home with permission but failing to use reasonable safeguards.
5. Providing a person served with information about another person served.
6. Sending faxed private information to an appropriate location but without appropriate protections, such as a confidential cover sheet.
7. Failing to report privacy and security violations.
8. Improper disposing of paper or electronic records.
9. Talking loudly about a person served, using their name, in a public area (lunchroom, reception area, in front of other persons served, etc).
10. Accessing the private information of a person served, who you used to work with, after they have transferred to another program out of curiosity about how the person is doing, and not in connection with ongoing services or other permitted purpose.
11. Posting information about persons served on social media.
12. Using or disclosing information about person's served in exchange for personal financial gain.

If you are found to be in violation, you may be subject to disciplinary action leading up to and including termination.

### **G. Individual Access to Private Data**

Individuals and/or their legal representatives have a right to access and review the individual's record. They also have the right to have the data explained.

1. A Rise team member will be present during the review and will make an entry in the person served's contact notes as to the person who accessed the record, date, and time of review, and list any copies made from the record.
2. An individual may challenge the accuracy or completeness of information contained in the record. Team members will refer the individual to the Complaints & Grievances policy for lodging a complaint or grievance.
3. Individuals may request copies of pages in their record.
4. No individual, legal representative, team member, or anyone else may permanently remove or destroy any portion of the person's record.

5. If the person served and/or legal representative objects to the accuracy of any information, team members will ask that they put their objections in writing with an explanation as to why the information is incorrect or incomplete.
6. 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 Complaints & Grievances.

#### **H. Case Manager Access to Private Data**

1. A person's case manager and the foster care licensor have access to the records of persons served by the program under section 245D.095, subd. 4.

#### **I. Requesting Information from Other Licensed Caregivers or Primary Health Care Providers.**

1. Complete the attached release of information authorization form. Carefully list all the consults, reports or assessments needed, giving specific dates whenever possible. Also, identify the purpose for the request.
2. Clearly identify the recipient of information. If information is to be sent to the program's health care consultant or other team member at the program, include Attention: (name of person to receive the information), and the name and address of the program.
3. Assure informed consent to share the requested private data with the person or entity has been obtained from the person or the legal representative.
4. Keep the document in the person's record.