



3195 Neil Armstrong Blvd.
Eagan, MN 55121
651-686-0405

204 Mississippi Ave.
Red Wing, MN 55066
651-388-7108

224 Main Street
Zumbrota, MN 55992
507-732-7888

1202 Beaudry Blvd
Hudson, WI 54016
715-410-4216

Reviewed 1/21/2021

Policy on Confidentiality

I-102

ProAct's policy on confidentiality is based on the Minnesota Data Practices Act and the Health Insurance Portability and Accountability Act (HIPAA). The purpose is threefold:

To protect the information that is obtained about persons served in order to provide services. ProAct requires an Authorization for Release of Information (ARI) form to be completed when information pertaining to persons served is requested of ProAct by other persons or agencies. ProAct also requires an ARI form when staff members request information from other persons or agencies.

To ensure the protection of vulnerable adults, respect individual privacy and the privileged status of confidential information, and report any maltreatment or exploitation.

To ensure that staff members will refrain from any type of social networking with individuals served which may breach the boundaries of professional conduct, and will refrain from favoritism to any individuals served.

The Data Practices Act, MN Statute 13.04, Subdivision 2, (Tennessee warning) states that: 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. This requirement shall not apply when an individual is asked to supply investigative data, pursuant to section [13.82, subdivision 7](#), to a law enforcement officer.

The HIPAA regulations cover standardization of electronic health, administrative and financial data and provide security standards protecting the confidentiality and integrity of individually identifiable health information, past, present or future.

ProAct Requests Information in order to:

- Determine eligibility for our services
- Provide effective services
- Enable us to collect public funding
- Confirm our license compliance
- Prepare statistical reports and evaluations
and/or financial audits
- Account for wages paid

The Minnesota Provider Notice of Privacy Practices explains:

- What data is being collected

- How ProAct will use the data
- If the participants is legally required to supply the data- or if he/she may refuse to do so
- Consequences for supplying the data or not
- Identity of other authorized persons
- Failure to give the warning is a violation of the law and may be used as evidence that ProAct is not in compliance with licensing rules.

Definitions:

- When the data on individuals is classified as ***Private***, the data is not accessible to the public- but is accessible to the participants and to authorized agencies.
- When data is classified as ***Confidential***, the data is not accessible to the public or to the participants, but is accessible to authorized agencies.

A Rule of Thumb:

- The Data Practices Act seeks to ensure that the public has access to all governmental data that is classified as ***Public*** and very limited access to data that is classified as ***Private*** or ***Confidential***.

If the Participants has Died:

1. Upon the death of a participants, all information about that person becomes ***Private***.
2. If the information was classified as ***Confidential***, then it remains ***Confidential***.
3. All Data Practices Act rights conferred on the participants become conferred on their living representative.

Who is Responsible for Enforcement?

The staff member at ProAct who is required to perform the duties necessary to implement and administer the Data Practices Act is responsible for enforcement. This person is the Corporate Compliance Officer.

However, staff members are responsible if they:

- Prepare procedures to assure access to the information
- Prepare an annual report to the public regarding the information
- Are responsible for limiting the amount of information collected
- Are responsible for storage (filing) of the data
- Are responsible for setting the procedures for collecting information.

During the intake meeting, each new individual entering ProAct will be informed and will sign off on the notice which describes how medical, health and related information about you may be used and disclosed and how you can get access to this information.

If you are a minor, you have the right to request that private data about you be kept from your parents. You must make this request in writing. You must explain why you wish this data to be withheld and what you expect the consequences of this activity will be. If ProAct agrees that withholding the information from your parents is in your best interests, it will not be shown to your parents.

ProAct will share information only when program services require access. The request must be made in written form to ProAct to ensure data privacy and accountability for the agency. We may share information with:

- State Department of Human Services
- State Rehabilitation Agencies (VRS, DVR, SSB)
- County Health & Human Services Staff and Board
- State Regional Services Center
- Persons, agencies, institutions, organizations or other entities under contract to one of the above, only to the extent of the contract.
- CARF
- US &/or MN Department of Labor
- Residential Providers
- Other Rehabilitation/Habilitation Providers
- Insurance Companies
- Employers
- Mental Health Service Providers
- Community Health/Mental Health Services Providers

Information will also be shared under the following circumstances:

- When you authorize sharing of information via a written release;
- To law enforcement personnel regarding criminal or civil proceedings relating to the administration of a program;
- Under court order;
- In an emergency.

By law, some government and contractor agencies have access to certain information about you if they provide a service to ProAct which requires access to your records. These include:

- U.S. Department of Health and Human Services
- U.S. Department of Labor
- U.S. Department of Agriculture
- U.S. Department of Social Security Administration
- MN/WI Department of Jobs and Training
- MN/WI Department of Economic Security
- MN/WI Department of Labor and Industry
- MN/WI Department of Revenue
- MN/WI Department of Veteran's Affairs
- MN/WI Department of Corrections
- MN/WI Department of Human Rights
- MN/WI Department of Human Services
- State, county or local health departments and other health care providers;

- MN Attorney General, county attorney or other law enforcement officials for program purposes;
- Creditors
- School districts, if necessary for program purposes;
- Community food shelves or commodity programs;
- Relatives who may be financially responsible for you;
- Interdisciplinary team members;
- Legislative auditor, state and federal program auditors;
- Parents, guardians, conservators, persons with power of attorney.
- Community Health/Mental Health Services
- WI Department of Health Services
- ContinuUs

Most data we maintain about you is **private**. You may view the data at ProAct if you make a written request to do so at least 24 hours before you wish to view it. A staff person will be present while you review the file. Data will not be shown to you if it is classified as **confidential**.

If you want to challenge the accuracy and completeness of information in your file, notify your assigned professional staff. You will be notified of data correction or that data is believed to be correct within 30 days.

You have the right to:

- Know what information is maintained about you;
- To view all public and private information about you;
- Authorize other persons to view data;
- Request copies (payment of the cost of copying required);
- Challenge the accuracy or completeness of records;
- Insert your explanation of anything you object to in your records;
- File an appeal of decisions made by the responsible authority.

OMBUDSMAN'S RIGHT TO ACCESS RECORDS

The ombudsman may examine, on behalf of a participants, records of an agency, facility, or program if the records relate to a matter that is within the scope of the ombudsman's authority. If the records are private and the person is capable of providing consent, the ombudsman shall first obtain the person's consent. The ombudsman is not required to obtain consent for access to private data on persons with mental retardation or a related condition. The ombudsman is not required to obtain consent for access to private data on decedents who were receiving services for mental illness, mental retardation or related conditions, or emotional disturbance.