SELECT HOME CARE SERVICES, INC.

DATA PRACTICES

I. What is Data Privacy and Why Is It Important?

In order to provide high quality, comprehensive services to people with disabilities within a licensed or regulated program, much information is needed. This information takes on many forms, such as medical data, social and family histories, professional evaluations, behavioral data, functional skill assessments, performance data for skill training programs, etc. When used appropriately, this information helps team members make well-considered decisions concerning the person's care and treatment.

Much of the information collected and maintained is very detailed and very personal in nature. Privacy issues are complicated by the fact that there are many people and many agencies involved in delivery of services for people in licensed programs. Assuring access to people and agencies that have legitimate need for information while at the same time protecting the individual's right to privacy and control over personal information becomes a significant challenge.

II. The Minnesota Government Data Practices Act.

In Minnesota, the Minnesota Government Data Practices Act, passed in 1979 and formerly called the Data Privacy Law, regulates information handling all government agencies and private agencies, which are licensed by the state. The Act has two main purposes:

To insure that individuals are given certain rights when a agency collects, stores, and uses information about them, and

To facilitate access to the information which should lawfully be disclosed?

For purposes of this training, we will focus on the handling of information of people with disabilities being served by licensed programs. The concepts and procedures we will review are:

Data Privacy and Confidentiality,
Privacy Rights Notices (sometimes known as Tennessean warning)
Authorization for Release of Information
Informed Consent
Emergency Situations
Client Access to Client Records

III. Data Privacy Confidentiality

Let's begin by discussing how data privacy and confidentiality affect staff in programs serving people with disabilities.

The first thing to be aware of is that persons receiving services have the right to expect that all personal information regarding them be kept confidential. Safeguarding this right is the foundation for mutual respect between the person receiving services and the staff.

Programs should only collect data that is genuinely needed. This includes data that is mandated by law or applicable rules and regulations and data that is needed to provide appropriate services.

It is each staff person's responsibility to make sure that the individual information they collect and record is complete, accurate, current, and necessary. This includes client/employee timecards and daily notes if taken. The timecards and notes contain personal and identifying information. They are to remain in the client's home until they are mailed into the agency. Employees *may not* bring timecards/notes home with them or keep them in their car.

Data privacy refers to all information on persons receiving services gathered for program purposes, including their presence or status in the program.

In other words, if someone telephones the program and asks if a certain person is a part of their program, this is considered private information and should not be given out unless you have valid authorization. Likewise, if someone who works in another agency asks if you work with a certain person, you should tell him or her that is private information, which you can't give out. This

sometimes happens when a person moves from one agency to another. It may seem harmless enough at first, casual talking about a person receiving services with someone who isn't involved in working with them, can invade the person's privacy.

Preserving confidentiality and protecting data privacy refer to both written and verbal exchanges. Discussions and conversation about a person receiving services should occur only in the line of duty.

It's not uncommon for staff to socialize during off-duty hours. Since it is common for staff to socialize during off-duty hours, and the job is a primary bond, it is quite natural in these situations for discussions about work to occur. Confidentiality problems can arise when co-workers discuss experiences with persons receiving services in public places where they can be overheard. For example, you are sitting in a booth in a restaurant talking with your co-workers about John Smith's latest behavioral incident and his cousin from out of town is in the next booth and overhears your conversation. This is a clear violation of data privacy and confidentiality. It is the responsibility of all staff members to keep client information safe. All information regarding your clients is considered personal and should not be shared. Identifying information must not be shared; this includes their name, where they live, their diagnosis etc. Select Home Care suggests that you do not discuss your client with anyone other than office staff. We also suggest that you do not share personal information about yourself with your client.

As a general rule, if you have any doubts about whether sharing certain information violates confidentiality, first ask your supervisor.

IV. Privacy Rights Notice (Tennessean Warning)

Whenever a person receiving services (or their legal representative) is asked to provide private or confidential information about themselves, they must have information about how that data will be used. The privacy rights notice gives some basic information about routine use of data and data sharing within the program and service delivery system. This notice does not take the place of informed consent and signed authorizations to release specific information. We will discuss these later. The privacy rights notice is sometimes referred to as the Tennessean Warning after the Act's initial author, Senator Robert Tennessean of Minneapolis.

A privacy rights notice must contain the following components:

The purpose and intended use of requested data within the agency or statewide system.

Whether the individual may refuse or is legally required to supply the requested system.

Any known consequences for supplying or refusing to supply data.

The identity of other persons or entities authorized by a state or federal law to receive the data.

In most agencies, a printed privacy rights notice is provided to the person receiving services upon admission and is updated periodically thereafter, usually annually. The notice should be explained to the person in terms that he/she can understand. The form is then signed by the person, or legal representative, and placed in the person's permanent record. A copy is given to the person and his/her legal representative.

V. Authorization for Release of Information

In addition to the fairly general privacy rights notice discussed earlier, further safeguards need to be taken whenever specific information is requested.

A. Conditions for Release of Information
Before information regarding a person receiving services can be given out, the following must be assured:
The person or their legal representative must give consent.

Data Practices

The consent must be voluntary. There must be no use of coercion or threats in order to get a person receiving services or their legal representative to sign a release of information authorization.

Person receiving services or their legal representatives can choose to release only part of the requested information.

The "authorization to release information" form can be signed only by the person receiving services or their legal representative. (Make sure that the person signing has legal authority to do so. For example: for a person who is under state guardianship or other type of guardianship, the person's parent or family member may not be authorized to sign).

B. The Consent Form

The consent form should:
Designate who will get the information

Specify what information can be released.

Indicate who will release the information.

Specify the purpose(s) for use of the information both immediately and in the future.

Contain a reasonable expiration date, not to exceed one year.

Contain a statement, clearly specifying the rights of the person receiving services to revoke their permission to release this information.

If permission is later revoked, the written revocation should be attached to the original consent form or an oral decision to revoke the consent should be clearly noted, dated, and signed on the original consent form.

Contain a statement that this information is private and protected by the Minnesota Government Data Practices Act.

-Be written in plain English

-Be dated

VI. Informed Consent

Informed consent refers to the person's ability to voluntarily participate in a rational decision-making process regarding treatment or services and the ability to weigh the risks and benefits of the proposed treatment/services after being provided the information. Determining the person's ability or capacity for informed consent can be difficult to determine. Many programs rely on a recommendation from the person's physician or psychologist as to whether the person has the necessary capacity to understand all the consequences of their consent. This is typically conveyed to the interdisciplinary team who makes the overall judgment regarding the person's ability to consent. If the person is under guardianship or conservatorship, the legal representative is responsible for giving informed consent.

A. Requirements for Informed Consent
Informed consent is generally required for:

- The person's participation in research projects.
- Release of photos, videotaping, and multimedia projects.
- Reviewing Vulnerable Adult Incidents with Human Rights Committee.
- Release of personal record information
- Aversive or deprivation procedures.

- Psychotropic medication authorization

Before it is implemented, the proposed procedure, program, treatment, or use of the information must be explained to the person receiving services or their legal representative in terms they can fully understand.

B. Conditions for Informed Consent

The following conditions must by met:

- Consent is freely provided, not under duress.
- The condition of the person receiving services is clearly understood by the person or his/her legal representative.
- The reason for the authorization is completely understood by the person giving consent.
- Alternatives to the procedure, program, treatment/service, or use of information (if any) are explained and fully understood.
- Risks and benefits of the procedure, program, treatment, or use of information are explained and fully understood.
- Chances of success of procedures, programs or treatments are explained and fully understood.
- The consent is time-limited and in writing.

VII. Emergency Situations

The statute allows for release of information without informed consent when the health or safety of the person is clearly in jeopardy. Documentation required for releasing information under these circumstances includes:

- The date and time.
- The person or agency the information was released to.
- The reason for this release of this information.
- Why consent could not be obtained, and the specific information released.
- The name of the person who made the emergency release.

The person should be informed about the emergency release of information as soon as possible. Documentation of this should be made in the record of the person receiving services.

VIII. Access to Records

The law requires that persons receiving services or their legal representatives are allowed access to their records. The program can implement policies requiring written requests and approval for record review, and conducted in the presence of specified staff. Persons receiving services should be informed on their admission to the program of their right to review their records as well as any policies and procedures the program has for this. If a person receiving services is denied access to his/her record, the reason for denial must be documented prior to the person's written request for access. Persons receiving services or their legal representatives can challenge the accuracy or completeness of the information contained in the record. This is usually accomplished through the procedures established in the program's grievance policy.

IX. Additional References

The Key to Privacy, Data Privacy Office, Minnesota Department of Human Services, 444 Lafayette Road, St. Paul, MN 55155.