Confidentiality Policy

Last Revised: December 2022

Contents

I. Purpose 1
II. Principles 2
A. Respect for the Privacy and Best Interest of the Customer 2
B. Informed Consent 2
C. "Need to Know" and "Minimum Necessary" Standard 2
D. Compliance With Confidentiality Laws and Policies 2
III. Policy 3
A. Staff Training and Assurances 3
B. Types of Confidential Customer Information 3
C. Access to Confidential Customer Information 3
D. Disclosure of Customer Information 4
IV. Procedures 6
A. Staff Actions to Safeguard the Confidentiality of Customer Information 6
B. Measures to Safeguard the Privacy of Customer Records and Data 7
C. Accessing Records From Outside of the Agency 8
D. Informing Customers of Their Rights 8
V. Additional Information 9

This policy applies to aging and disability resource centers (ADRCs) and Tribal aging and disability resource specialists (Tribal ADRS), herein referred to as "agency" or "staff."

I. Purpose

The purpose of this policy is to provide guidance on how information should be accessed or shared consistent with the customer's right to privacy and with the requirements of state and federal law. The policy and procedures in this document are fundamental to any county or Tribal confidentiality policy that applies to the ADRC or Tribal ADRS. Agencies may have one confidentiality policy for their county or Tribe as long as the requirements in this policy are included in the county or Tribal policy.

All ADRC staff, including volunteers, board members, contractors, and Tribal ADRS are expected to be familiar and comply with the requirements of this policy. Benefit specialists are subject to the confidentiality requirements specific to their program and should follow their program guidelines when different from this policy.

II. Principles

A. Respect for the Privacy and Best Interest of the Customer

Decisions about what customer information is accessed or shared will be based on what is in the best interest of the customer and consistent with the customer's right to privacy. Customers should not be pressured to reveal more than they are willing to share and will be allowed to remain anonymous if they so desire.

B. Informed Consent

Customers should be told that the information they share with the agency is kept in confidence and may be shared, when needed, with the customer's permission. It is best practice to inform customers about how their information will be used and to obtain at least a verbal consent, even when consent is not strictly required.

If staff have reason to believe that the information the customer has shared or is about to share would not be protected, they should inform the customer of the limits to confidentiality. These include reporting abuse or neglect; cooperating with public health, adult protective services, law enforcement, or a court order; and emergency situations.

C. "Need to Know" and "Minimum Necessary" Standard

Staff shall obtain only that information which they need to know to assist the customer and will use customer information only for purposes directly related to the provision of services to the customer.

D. Compliance With Confidentiality Laws and Policies

Customer confidentiality is protected by federal and state statutes and regulations and by county or Tribal government policies and procedures. The agency and its staff will abide by all legal requirements relating to confidentiality.

III. Policy

A. Staff Training and Assurances

All newly hired staff will be trained on the confidentiality policy as part of their orientation. Refresher training will be provided to all staff annually.

All staff must sign a confidentiality and non-disclosure agreement stating that they have reviewed, understand, and will abide by the confidentiality policy before being given access to confidential customer information. A copy of the policy will be given to each staff member for their records, and a copy of the signed confidentiality agreement will be kept in each staff member's personnel file. This agreement shall be reviewed and signed annually, at a time determined by the agency.

B. Types of Confidential Customer Information

All personal information about a customer is considered confidential. This includes but is not limited to:

- The person's name, address, birth date, Social Security number, and other information that could be used to identify the customer.
- The person's physical or mental health, functional status, or condition.
- Any care or services that the customer has received, or will receive, from the agency or any other provider.
- Financial information, including income, bank accounts and other assets, receipt of benefits, eligibility for public programs, or method of payment for services provided to the customer.
- Employment status or history.
- Education records.
- Any other information about the customer that is obtained by staff.

C. Access to Confidential Customer Information

Staff, including directors and supervisors, may access confidential customer information to provide information and assistance, options counseling, benefits counseling, functional

eligibility determination, enrollment counseling, and other ADRC services.

D. Disclosure of Customer Information

Staff may not disclose or acknowledge whether a person has received or is receiving services from the agency, unless it has been established that the information can be legitimately shared. When unsure, staff receiving an inquiry regarding the status of a customer will respond in a non-committal manner. For example, staff may say, "The agency confidentiality policy does not permit the disclosure of that information."

1. Disclosures That Require Prior Written Informed Consent

The types of disclosures that require prior signed authorization from the customer or the customer's legal representative include:

- Information with counties outside of the agency's service area for purposes other than access to publicly funded long-term care programs.
- Medical information with an employer, life insurer, bank, marketing firm, news reporter, or any other external entity for purposes not related to the customer's care.
- Substance use disorder (SUD) treatment records.
- School records.
- Any disclosure for purposes not relating to the services provided by the agency.

2. Process for Obtaining Written Informed Consent

The agency will obtain a release of information form that describes the information to be shared and who can receive and use the information, and that is signed and dated by the customer whose information is to be shared or by their legal representative. A copy of the signed release form will be given to the customer or their legal representative.

The customer's records and a copy of the signed release of information form will be kept in the customer's file.

Any written disclosure of confidential information by staff will be accompanied by a written statement documenting that the information is confidential and that further disclosure without the customer's consent or statutory authorization is prohibited by

law.

3. When Verbal Consent Is Sufficient

The following situations require only verbal consent to share customer information:

- Sharing information with the customer's family, friends, caregivers, and providers who are involved with the person's care, when necessary to coordinate services for the customer.
- Contacting an agency or service provider on the customer's behalf.
- Referring the customer to services provided by the agency.
- Referring the customer to services provided by other county or Tribal departments or agencies.
- Linking customers to community resources.

Records of verbal consent should be documented and kept in the customer's file.

4. Customer Right to Revoke Consent

A written release of information or verbal consent may be rescinded by the customer or their legal representative at any time. This should be done in writing, if possible. Revocation of a prior consent should be documented in the customer's file.

5. Disclosures That May Be Made Without Written or Verbal Informed Consent

Neither written nor verbal informed consent is required in the following situations; however, it is advisable to let the customer know that these exchanges may take place when:

- Exchanging customer information necessary for the agency to perform its duties or coordinate the delivery of services to the customer.
- Transferring the long-term care functional screen for the purpose of enrollment into a managed care organization (MCO) or IRIS[1] consultant agency (ICA) in the

[1] IRIS stands for "Include, Respect, I Self-Direct".

agency's service area.

- Transferring the long-term care functional screen to the ADRC serving the county in which the customer resides.
- Exchanging information necessary to coordinate the delivery of ADRC services, county human services, Tribal services, social services, or community programs to the customer.
- Reporting possible abuse or neglect of an elderly person or vulnerable adult, per Wis. Stat. §§ 46.90 and 55.043.
- Cooperating with public health, adult protective services, or elder or adult-at-risk investigations.
- Cooperating with a law enforcement investigation. Check with your legal counsel before providing information in this type of situation, as there are limited situations where you can disclose information to law enforcement.
- Sharing information in the event of an emergency, per established emergency procedures.
- Exchanging information necessary for the Wisconsin Department of Health Services to administer the Family Care, IRIS, or Medicaid programs.
- Exchanging information necessary to comply with statutorily required advocacy services for Family Care and IRIS enrollees and prospective enrollees.
- Required by a signed court order.

IV. Procedures

A. Staff Actions to Safeguard the Confidentiality of Customer Information

Staff are expected to employ the following practices to safeguard customer confidentiality:

- Only access personal and identifiable customer information when you need it to perform your job.
- Disclose confidential information only to those who need it to complete their jobs and are authorized to receive it.
- Obtain informed consent prior to accessing or disclosing information, consistent with

provisions outlined in this policy.

- Do not discuss a customer's information with anyone else unless access to such information is expressly permitted by the customer.
- Do not access information about your family members, neighbors, or friends. Review any requests to serve people you know with your supervisor.
- Refrain from communicating information about a customer in a manner that would allow others to overhear.
- Keep confidential information out of sight.
- Protect access to electronic data.
- Send fax transmissions that contain confidential information with a cover sheet that includes a confidentiality statement.
- Delete or dispose of information that is outdated and no longer needed in accordance with record retention guidelines and state and federal laws.
- Report any violations of confidentiality to your supervisor.
- Check with your supervisor if you are unsure whether information may be disclosed.

B. Measures to Safeguard the Privacy of Customer Records and Data

In addition to the above guidelines for staff, the agency must have the following safeguards in place to protect the privacy of records and data and to prevent inappropriate use or disclosure of customer information:

- Locked file cabinets for confidential information and a secure area for records storage are provided.
- Confidential documents that are no longer needed are shredded.
- Staff computers are equipped with security features to protect customer data from unauthorized interception, modification, or access during electronic transmission and receipt, transfer, and removal of electronic media.
- Computers, laptops, and portable devices have encryption software installed.
- When disposing of printers, copiers, scanners and fax machines, the hard drives are wiped, or otherwise disposed of, in a way that prevents access to captured document images.

- Staff who leave their employment or affiliation with the agency lose their ability to access customer information and data systems, effective immediately upon their departure.

C. Accessing Records from Outside of the Agency

Customers or their legal representatives will be asked to sign a release of information form to permit the agency to access any confidential records needed to complete the long-term care functional screen or provide other services to the customer. The signed form will be kept in the customer's file and a copy of the signed form will be provided to the customer.

D. Informing Customers of Their Rights

1. Informing Customers About the Confidentiality Policy

As a common practice, staff will ask customers whether they have any objection to sharing information, even if written authorization is not required. Staff will inform customers about the agency's confidentiality policy and the customer's right to see their records, obtain copies, and contest the information contained in those records.

2. Customer Requests to View or Get Copies of Their Records

Customers have a right to view and receive copies of their records on file at the agency. To do so, the customer or their legal representative will submit a written request, a copy of which will be kept in the customer's file, together with a record of the information that was disclosed. The agency may charge the customer for paper copies of records exceeding 10 pages.

3. Requests to Share Agency Information with a Third Party

If the customer wants information from their record given to another person or agency, the customer or their legal representative must complete a release of information form indicating which information is to be sent and to whom. The agency may charge the customer for paper copies of records that exceed 10 pages.

E. Monitoring and Ensuring Compliance

Supervisors are responsible for monitoring and ensuring staff compliance with this

confidentiality policy by conducting periodic compliance checks, reviewing the confidentiality policy with annually with staff, and providing training to staff.

1. Reporting Security Violations and Breaches of Customer Confidentiality

Staff will report any breach of customer confidentiality to their supervisor or privacy officer as soon as it is discovered and follow the designated incident reporting process, where applicable. The ADRC director or supervisor should report the breach to their assigned regional quality specialist for awareness.

2. Mitigating and Correcting Breaches of Confidentiality

Violations of the confidentiality policy will be documented and corrected. Where required or appropriate, customers will be notified of the breach and of actions taken to mitigate the situation.

V. Additional Information

If you have questions or would like additional information, contact your assigned regional quality specialist.

Confidentiality and Non-Disclosure Agreement — ADRC Representative

As a representative of the Aging and Disability Resource Center of _____, I have reviewed and received training on the confidentiality policy. If I do not fully understand this policy or how it is relevant to my employment or association with the ADRC, I will not sign this statement until I have spoken with the ADRC supervisor and I understand this policy.

I acknowledge that I will be required to review the confidentiality policy on an annual basis.

As a representative of the ADRC, I acknowledge, by signature, that I have reviewed the confidentiality policy, received training on the policy, and agree to comply with its provisions. I acknowledge the obligation of ADRC staff to protect the confidentiality of ADRC customers in accordance with this policy.

Printed name and title:

Date of policy review:

_____ _____

Signature: Date signed:

_____ _____

Supervisor Signature: Date signed:

Confidentiality and Non-Disclosure Agreement — Tribal ADRS

As a Tribal Aging and Disability Resource Specialist for the _____, I have reviewed and received training on the confidentiality policy. If I do not fully understand this policy or how it is relevant to my employment or association as a Tribal ADRS, I will not sign this statement until I have spoken with my supervisor and I understand this policy.

I acknowledge that I will be required to review the confidentiality policy on an annual basis.

As a Tribal ADRS, I acknowledge, by signature, that I have reviewed the confidentiality policy, received training on the policy, and agree to comply with its provisions. I acknowledge the obligation of the Tribal ADRS to protect the confidentiality of Tribal ADRS customers in accordance with this policy.

Printed name and title:

Date of policy review:

_____ _____

Signature: Date signed:

_____ _____

Supervisor Signature: Date signed: