Section 1.7: Data Privacy

MAY 2019

References

7 CFR 246.26 (d-h)

> **(d)(1)(i-ii)"Confidentiality of applicant and participant information** —
>
> (1) WIC purposes. (i) Confidential applicant and participant information is any information about an applicant or participant, whether it is obtained from the applicant or participant, another source, or generated as a result of WIC application, certification, or participation, that individually identifies an applicant or participant and/or family member(s). Applicant or participant information is confidential, regardless of the original source and exclusive of previously applicable confidentiality provided in accordance with other Federal, State or local law. (ii) Except as otherwise permitted by this section, the State agency must restrict the use and disclosure of confidential applicant and participant information to persons directly connected with the administration or enforcement of the WIC Program whom the State agency determine have a need to know the information for WIC Program purposes. These persons may include, but are not limited to: personnel from its local agencies and other WIC State or local agencies; persons under contract with the State agency to perform research regarding the WIC Program, and persons investigating or prosecuting WIC Program violations under Federal, State or local law."

MN Statute 13.01-13.99

Policy: Local Agencies must protect and secure private WIC participant data at all times and may not disclose or release private data except under certain circumstances following specified procedures as outlined below.

Purpose: Individual WIC applicant/participant information is **private**. This policy exists to maintain privacy and to protect the integrity of participant data.

Definitions (from MN Statute 13)

Private data on individuals are data made by statute or federal law applicable to the data: (a) not public; and (b) accessible to the individual subject of those data.

Summary data means statistical records and reports derived from data on individuals but in which individuals are not identified and from which neither their identities nor any other characteristic that could uniquely identify an individual is ascertainable.

Procedures

To ensure data privacy, Local Agencies must:

- Secure WIC participant data (paper records and/or electronic data) at all times, including during collection, printing, storage, and transport.
- Limit the release or sharing of private WIC data to instances in which the participant, custodial parent or legal guardian has provided signed consent to release such data and other instances as required by law.
- Provide annual training on data security to Local Agency staff and maintain documentation of the training. (See Security Training)
- Gather information in a private space so that others cannot hear.
- Allow time for participant/caregiver to read (or be read to) the Rights & Responsibilities; inform them how information might be used (Exhibit 1-K); and obtain signature from participant/caregiver regarding their acceptance of the Rights and Responsibilities.
- Protect participant private data and do not share except as allowed by law or authorized by the participant.
- Use appropriate security at clinic (see Section 9.3: Security of WIC Information System)
- Ensure that private data sent via email is appropriately encrypted, encoded, or protected.

Releasing information: Private WIC data may only be released under certain circumstances

1. WIC data may be viewed and used by persons directly working with the administration, monitoring, or enforcement of the WIC Program, including local, state, and federal WIC staff. Aggregate or summary WIC data is considered public and may be used for a variety of purposes.
2. Private data may be released to other parties only with the written consent of the participant, custodial parent, or legal guardian. Written consent is obtained by asking the participant, custodial parent, or legal guardian to complete a Consent to Release Information form. These forms should be limited to authorize the release of data for continuity of care and for the benefit of the participant. WIC private data shared with appropriate consent may not be released to a 3rd party without written consent or authorization.

A Consent to Release Information **must** include:

- Name of the participant for whom the data applies
- What data is being released
- The purpose for releasing the data/how the data will be used

- To whom the data is being released (including name(s) of specific programs or providers rather than entire organizations so that participants can select appropriate recipients of the private data and choose not to select any programs they feel are not appropriate recipients)
- Notification that declining to sign the release will not impact the individual's eligibility or participation in the WIC Program and that individual data will not be shared
- A statement of the individual's right to revoke the authorization in writing
- Signature of the participant, custodial parent, or legal guardian
- An expiration date

A Consent to Release Information **must not** include:

- Pre-checked boxes indicating broad entities with which to share the individual's data, but rather, complete in an individualized way to meet the needs of each individual participant for care coordination and continuity of care and ensure the participant understands they can choose which programs with which sharing can occur and which programs no sharing can occur.

An example form for Consent to Release Information can be found in Exhibit 1-C: Sample Authorization for Release of Information

To ensure that there is no inferred coercion, release forms for private physicians or other health care providers may be included as part of the WIC application or certification process; however, all other requests to sign voluntary release forms must occur after the application and certification process is completed.

3. Exceptions when private data may be released without the written consent of the participant, custodial parent or legal guardian:

   - Information regarding suspected or known child abuse or neglect must be released to the proper authorities according to the law (The Federal Child Abuse Protection and Treatment Act).
   - A court order is required for the release of private data without a signed consent. If a search warrant or a court order is presented, local agency staff must notify the State Agency, and consult with their legal counsel for advice regarding how to respond and seek to limit the disclosure. A subpoena is not adequate for disclosure of private data.

Data Breach: An unauthorized disclosure of private WIC data

Private data is accessible to the subject of the data but is not accessible to the public. Some examples of a data breach include, but are not limited to:

- Lost or stolen bag, paper participant files/charts, removable storage device containing private data.
- Lost, stolen, or hacked laptop or desktop containing private data.
- Misguided or misaddressed email, post mail, or fax containing private data.

- Any other situation in which an unauthorized person has access to private data.
- There are many other ways that data security can be breached. If you are unsure of whether a data breach has occurred, always report the incident, and see further guidance.

Report Data Breaches (or Suspected Data Breaches) Immediately

If you see or experience a breach or potential breach of private data, you must **immediately notify** the proper authority in your Local Agency that oversees private data and the State WIC Consultant.

It is the Local Agency's responsibility to work with their administrator/legal unit and the State Office to determine who else to contact and what actions to take. Information you provide regarding a data breach will be used to stop the breach, mitigate any problems, and possibly for investigative purposes.

Contact the State WIC office with the following information:

- Agency name and number
- List of missing equipment
- Location where loss/theft occurred
- Date and time loss/theft occurred (actual, if known, or estimated)
- Date and time loss/theft was discovered
- Circumstances involved
- Provide a copy of the police report information, if applicable
- Name and telephone number of staff person to contact with questions

Guidance

- If there is any uncertainty about the identity or authorization of an individual requesting access to private data, seek valid identification of the individual to ensure appropriate authorization.
- When working outside the main office, take only materials and records that are needed.
- When using a shared printer, collect copies immediately.
- Safeguard private data when communicating with participants outside of WIC clinic. Private data is described in MN Statute 13.01-13.99, including any information that would imply an individual's application to or participation in the WIC program.

Mail and Telephone

- If mailing information, WIC identifiers should not be visible on an envelope or on the outside of a postcard including the return address (using Public Health Address is permissible).
- If calling participants, confirm phone number at appointments and document any special instructions for leaving messages with others or on voice mail.

- Give participants the opportunity to opt out of this type of communication. Document in the WIC Information System if the participant does not want to receive mail or telephone communication.

Text and Email

- Minnesota Department of Health recommends obtaining written authorization prior to sharing any non-public data by email or text. The consent form should include a warning that sending information by text/email is not secure and provide the participant the opportunity to revoke the release at any time (See MOM Exhibit 1-C-Sample Authorization for Release of Information). Agencies are encouraged to consult with their county attorney or data privacy officer regarding these methods of communication.
- An appointment time and personal/individualized nutrition or breastfeeding information is considered private data.
- Education materials, such as nutrition education cards, are not considered private data and can be mailed (see mailing above), texted or emailed. Any materials posted on the WIC website are considered public information.
- If an agency is using a third-party vendor for text messaging, the consent for that texting service is adequate. It is not necessary to obtain an agency-specific secondary consent for that texting service.

Contact your State WIC Consultant with any questions and for further guidance.

Reference – Complete Listing of Hyperlinks

7 CFR 246.26 (d-h) (http://www.gpo.gov/fdsys/pkg/CFR-2012-title7-vol4/pdf/CFR-2012-title7-vol4-sec246-26.pdf)

MN Statute 13.01-13.99 (https://www.revisor.mn.gov/statutes/?id=13)

Security Training (https://www.health.state.mn.us/people/wic/localagency/infosystem/hubert/training/index.html#security)

Exhibit 1-K: Rights and Responsibilities (https://www.health.state.mn.us/people/wic/rights.html)

Section 9.3: Security of WIC Information System (https://www.health.state.mn.us/docs/people/wic/localagency/program/mom/chsctns/ch9/sctn9_3.pdf)

Exhibit 1-C: Sample Authorization for Release of Information (https://www.health.state.mn.us/docs/people/wic/localagency/program/mom/exhbts/ex1/1c.pdf)

Minnesota Department of Health - WIC Program 625 Robert St N, PO BOX 64975, ST PAUL MN 55164-0975; 1-800-657-3942, health.wic@state.mn.us, www.health.state.mn.us. To obtain this information in a different format, call: 1-800-657-3942

This institution is an equal opportunity provider.