Section 9.6: WIC Electronic Communications Security

MAY 2024 - DRAFT

References: MN Statutes Ch 13 MN Data Practices Act; 7 CFR 246.26 (d-h); Telephone Consumer Protection Act 47 U.S.C. § 227; Secure and Trusted Communications Networks Act of 2019, 47 U.S.C. § 1601(b)(2)(A)-(C).; Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. 115-232 (Aug. 13, 2018); Minnesota Information Technology (MNIT) Services: Prohibited Technologies Policy, Prohibited Technologies Standard

Policy: Electronic communication (such as: email, text, etc.) between Local Agencies and WIC participants may only be conducted with permission from the participant and appropriate safeguards must be in place when the communication involves private data.

Purpose: Local Agencies use electronic methods of communication with participants such as texting, emails, faxes and the Mobile Management system. Local agencies must ensure that communication methods are secure when private data is shared by the local agency.

The following are procedures for ensuring the security of communications.

Procedures

Email Communications

Email communications are generally not considered a secure form of communication for private information.

To ensure participant privacy, the Local Agency must work with local partners (IT and Legal) to ensure the Local Agency is using a secure locally approved process to send a secure/encrypted email when communicating private data via email with participants.

- The Local Agency should **NEVER:**
  - Use personal staff email addresses (e.g.; @gmail.com) to communicate with participants.
  - Save emails with private data in the agency's network folders accessible to non-WIC staff.

Emails should only be kept for the minimum amount of time needed for business purposes and then deleted. (See Section 1.7: Data Privacy)

Text Message Communications

Text messaging is **NOT** considered a secure form of communication. Although a texting platform may indicate they are HIPAA compliant, it is the Local Agency's responsibility to ensure the participant's data is kept private and to follow Local Agency IT and Legal requirements.

If the Local Agency is using a texting platform

- The Local Agency **MUST:**
  - Receive and document the participant's permission to receive text messages. (See Section 1.7: Data Privacy)
    NOTE: documented permission is not required to use texting via the WIC Mobile Management system, to use the "Contact Us" feature in the My MN WIC Mobile App the participant must Opt-In for text messaging to use the feature.
  - Ensure text messages are easy to understand and do not contain abbreviations.
  - Delete text messages immediately after viewing.
- The Local Agency **MUST NOT:**
  - Send private information via text message.
  - Text a participant using a staff members personal cell phone.
  - Save a participant's name to personal or Local Agency issued phone contacts list.
  - Use free versions of texting services.
  - Use an iPhone, unless it is ensured that iMessages are turned off, as these are automatically saved to an iCloud account.
  - Request that a participant send any of the following via text:
    - Personal Health Information
    - Identifiable data such as social security or driver's license numbers
    - Photos or proofs for certifications with personal information
- If a participant wants to submit personal information via text message the Local Agency **MUST** inform the participant that it is not considered a secure way to submit information and offer alternate ways to submit the information electronically (See Guidance).

Fax Communications

There are multiple ways a Local Agency may receive a Fax communication. The Local Agency is responsible for ensuring that transmission of the service they are using is private and secure and only appropriate WIC Staff have access to private participant information. Prior to

implementing, the Local Agency should confirm with their Local Information Technology (IT) staff if the service they plan to use is considered private and secure.

The following faxing technology is **NOT** considered private and secure:

- A centralized shared fax machine used by multiple programs

The following faxing technology **may be** considered private and secure; confirm with Local IT:

- A business unit fax machine used only by Local Agency WIC staff
- VSI-Fax maintained by Local Agency Information Technology staff
- eFax maintained by Local Agency Information Technology staff

WIC Mobile Management Portal "Contact Us" feature and text messaging

Mobile Management is a browser-based application that can be used by Local Agency staff to directly communicate with WIC participants via text message and obtain documentation in a secure way. This communication is initiated by WIC participants using the Contact Us feature in the My MN WIC App.

- For participants to use the Contact Us feature within the My MN WIC Mobile app they must opt-in to text messaging. This consent is only for texting that occurs between the participant and the Mobile Management Portal. If the Local Agency is using another texting platform an additional release for texting must be signed (See Section 1.7: Data Privacy).
- **NEVER** request that a participant send images or documents via a text message that contains personal information in the WIC Mobile Management Portal. The participant should be directed to start a new Contact Us contact and use the "Submit Documents to WIC" option; this process is considered secure.
- **NEVER** send a text message response that includes private information.

Ban on Purchase of Select IT items

Local Agencies MUST ensure that Federal funds are NOT used to purchase, either directly or indirectly, any IT related product(s) or service(s) from any vendor indicated as prohibited by the Secure and Trusted Communication Networks Act of 2019 and Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. 115-232 (Aug. 13, 2018).

- Information is also reflected in the WIC Grant Agreements and is written as follows:

  By signing this agreement Grantee certifies that, consistent with Section 889 of the John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. 115-232 (Aug. 13, 2018), Grantee does not and will not use any equipment, system, or service that uses "covered telecommunications equipment or services" (as that term is defined in Section 889

of the Act) as a substantial or essential component of any system or as critical technology as part of any system. Grantee will include this certification as a flow down clause in any contract related to this agreement

The following link to resources containing the prohibited vendors list for IT related products and services:

- Federal Communications Commission (FCC) List of Equipment and Services Covered By Section 2 of The Secure Network Act
- Minnesota IT (MNIT) Services Prohibited Technology Standard

Guidance

Text Message Release of Information

Local Agency staff may obtain an initial verbal temporary consent to communicate via text messaging with documentation in the state use field in the Information System. A written release of information with a signature consent for text messaging **must** then be obtained at the next participant contact and be scanned/uploaded into the Information System.

The Local Agency may create their own texting specific release of information. This release **must** include the following statement:

- *I understand that sending information electronically may not be secure. I assume the risk that persons other than the intended recipient may observe information sent by these media. Depending on my phone plan, there may be charges I will be responsible for, and I can ask to stop receiving these types of communication at any time.*

Suggested text communication usage

The following are suggested uses for text messaging:

- Scheduling appointments and appointment reminders that do not include names
- Inviting participants to phone calls
- Sending links to food or nutrition resources

Secure document submissions

The following are considered secure ways to submit documentation electronically:

- My MN WIC Mobile App “Contact Us” feature
- Minnesota WIC Participant Documents Submission Form
- Minnesota WIC Online Application
- Secure or Encrypted emails

Reference – Complete Listing of Hyperlinks

Prohibited Technologies Policy
(https://mn.gov/mnit/assets/Prohibited%20Technologies%20Policy_tcm38-566880.pdf)

Minnesota IT (MNIT) Services Prohibited Technology Standard
(https://www.health.state.mn.us/docs/people/wic/localagency/prohibtech.pdf)

Section 1.7: Data Privacy
(https://www.health.state.mn.us/docs/people/wic/localagency/program/mom/chsctns/ch1/sctn1_7.pdf)

John S. McCain National Defense Authorization Act for Fiscal Year 2019, Pub. L. 115-232 (Aug. 13, 2018)
(https://uscode.house.gov/statutes/pl/115/232.pdf)

List of Equipment and Services Covered by Section 2 of The Secure Networks Act
(https://www.fcc.gov/supplychain/coveredlist)

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