Security Training 1 – Data Security, Privacy, Breaches, and Cybersecurity Incidents

SCRIPT - REVISED MARCH 2026

Introduction

Welcome to the Security Training 1 module – Data Security, Privacy, Breaches, and Cybersecurity Incidents.

This training is for all MN WIC Program staff and is provided by the MN Department of Health WIC Program.

Overview 1

The purpose of these data security training modules is to ensure all WIC program staff are familiar with the security requirements and responsibilities associated with safeguarding participant information and accessing and using the WIC information system.

Overview 2

After reviewing these training modules, we should understand and recognize security expectations and requirements, our responsibilities for maintaining participant privacy and protecting the confidentiality of participant data, as well as how by practicing appropriate security measures we can protect ourselves from potentially contributing to security breaches.

Overview 3

In this module, we'll take a look at data privacy and confidentiality, when and how we can share WIC data, and what constitutes a data breach and cybersecurity incident.

Data privacy

WIC data is confidential

Participation in WIC is voluntary but to fully assess eligibility and referral needs, it requires our participants to disclose private (confidential) data.

Federal regulations require we ensure strict confidentiality of WIC data.

Knowledge check 1

What do you know?

Whether a person has **applied** to participate in the WIC Program is private information. True or false.

Private and confidential

Any information that can be used to identify an individual person or **relates to** an applicant, participant, or family member(s) is **confidential,** which is referred to as "private data" in Minnesota State Law.

This includes, but is not limited to, names, contact information, health data, appointment information, and whether they have applied to participate or are participating in the WIC Program.

Click the button to continue.

Knowledge check 2

What do you know?

It is OK to ask a co-worker if they can get a measurement of a baby for us, referring to the infant by their full name, in a room where other WIC participants are waiting for an appointment because the infant is participating in WIC as well. True or false.

Unintentional disclosure

In clinic, we should always endeavor to provide both visual and auditory privacy when collecting or sharing confidential information.

We should use non-private references when mentioning or discussing participants if we can't be 100% certain we won't be overheard and potentially expose private information.

For example, "Can you help me measure the baby in room 2B?"

Sharing WIC data

Knowledge check 3

What do you know?

A Release of Information (ROI) allowing a participant's WIC information to be shared with a texting platform must be obtained only **after** the application and certification process have been completed. True or false.

Release of information 1

WIC regulations generally prohibit sharing WIC data with third parties without a written release of information (ROI).

The ROI must be signed by an individual who has legal authority to consent – for example, the participant, a child's parent, guardian, or other authorized individual.

ROIs must be obtained only **after the application and certification process is complete** to ensure there's no implied pressure or undue influence to sign it.

We must make it clear to the participant that signing the ROI is voluntary and optional.

Exception

While release of information (ROI) forms are typically completed after the WIC application or certification process, an important exception exists.

As part of the initial application or certification, we may include release forms that authorize the program to request specific health information from health care providers, such as anthropometric measurements, bloodwork results, or medical formula needs.

Knowledge check 3A

What do you know?

A Release of Information (ROI) signed by a person authorized to consent must be obtained to provide a WIC hemoglobin measurement to a health care provider requesting the information for a patient participating in the WIC Program. True or false.

Release of information 2

Signed forms that obtain written consent to authorize release of information or data are required to share a participant's name and/or personal information with any person or entity **outside of the WIC Program.**

ROIs should be primarily used for continuity of care and for the participant's benefit.

Consent

If there is a question or dispute about who has legal authority to consent to the release of information, WIC staff should require written proof of custody and inform the WIC coordinator/supervisor and, if appropriate, legal counsel.

Consultation with legal counsel is especially important in situations involving custody/guardianship disputes or child protection matters.

If we are still uncertain about the legal authority to consent, we must consult state WIC staff.

Knowledge check 4

What do you know?

We can export an Infoview report and share its output with another agency as long as the agency requesting the data is a public health program. True or false.

Sharing data – other programs 1

To comply with federal WIC regulations WIC data must be protected and not shared with other Health and Human Service programs without an authorized consent to release information by individual participants.

Our goal is to ensure participant's data is protected while still providing them with access to programs for which they are potentially eligible.

Knowledge check 5

What do you know?

We can share private information for currently certified Minnesota WIC participants with another state WIC agency (ex: Maine) if they call to obtain the certification information for a transferring family. True or false.

Sharing data – other WIC states

Per federal regulations, 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.

This means we can share WIC information with other state WIC agencies without a consent to release information.

Knowledge check 6

What do you know?

Because we are a public health program, we are legally obligated to provide WIC information if requested by the police. True or false.

Sharing data - authorities 1

If local authorities request private data, we **cannot disclose that information** without a signed consent from someone with authority to sign that consent.

Sharing data - authorities 2

A **court order or search warrant** is required for the release of private data without a signed consent from an individual authorized to provide this consent.

If a court order or search warrant is presented, **it must explicitly grant access to specific WIC confidential data, and we must notify the local agency's legal counsel and the State Office for advice regarding how to comply with the warrant and seek to limit the disclosure.**

Subpoenas are generally not adequate for disclosure of private data.

Knowledge check 7

What do you know?

We do not need a signed consent by someone with authority to release private data when reporting that we suspect or have identified child abuse or neglect. True or false.

Exception – reporting abuse/neglect

If we personally suspect or identify child abuse or neglect, we may disclose or provide information to the proper authorities according to the applicable state and federal laws and regulations without first obtaining a written consent to release information.

We should follow our local agency policy on how to report this.

Sharing data summary

If we receive a request to share data or have questions or concerns about whether an individual has legal authority to consent to release of information, we should always discuss these requests/questions/concerns with our WIC coordinator or supervisor **before** responding to the data request.

Our state WIC consultant is also always available to assist us.

Data breaches

Knowledge Check 8

What do you know?

An unauthorized or **unintentional** disclosure of private data is a data breach. True or false.

Definition

A data breach is any situation in which an unauthorized person has access to private or confidential WIC data.

Examples

Some examples if they contain participant information include, but are not limited to:

providing information without a release of information from the participant or a person authorized to consent to release of that information; sharing information without a court order or search warrant explicitly granting access to specific WIC data; lost, stolen or hacked computer, phone, tablet or other technological hardware; lost or stolen reports or papers; and misguided or misaddressed email, post mail or fax.

Knowledge check 9

What do you know?

We should wait to confirm that a data breach has occurred before contacting the WIC state office. True or false.

Reporting data breaches

Data breaches must be taken very seriously and whether we are certain or not as to whether it has occurred, if there is any chance, we must report it to the state office immediately.

We should inform our WIC coordinator or supervisor, the WIC MIS & Data supervisor, the WIC Nutrition & Clinic Services supervisor, and our state WIC consultant.

Information to provide

We must also provide the following information: our agency name and ID; a list of the missing equipment or participant data, etc.; the location of the loss, theft, or unintended disclosure; the date and time (actual if known or estimated); the circumstances involved; and a copy of the police report if applicable.

Data breaches

The repercussions of losing or exposing private data cannot be exaggerated and can be far-reaching.

It is our WIC agency's responsibility to work with the state WIC office and their administrative or legal unit to determine who else to contact and what actions will need to be taken.

The information we provide will be used to stop the breach, mitigate any problems, and possibly for investigative purposes.

Cybersecurity incidents

Knowledge check 10

What do you know?

An example of a cybersecurity incident is a WIC staff person clicking on a link that results in a ransomware demand. True or false.

Cybersecurity incidents 1

Cybersecurity incidents include but are not limited to malware or ransomware infections, unauthorized access to system or user accounts, phishing or credential compromise involving WIC users, network intrusions or security breaches, and any cyber incident that may involve exposure of private participant data.

Recognize

We need to recognize that we have the power to protect ourselves from cybersecurity incidents.

Phishing, malware, and ransomware scams often arrive as urgent emails or texts that try to trick us into clicking an unsafe link or opening an attachment.

We should always verify unexpected messages and avoid downloading unknown files.

Ensuring our computer software is up-to-date will also help keep us safe from potential cybersecurity incidents.

Avoid

Avoiding potential cybersecurity incidents starts with treating every unexpected message, link, or attachment as potentially unsafe.

Some common tricks are instilling a sense of urgency or fear in us by sending messages claiming an account will be impacted, a payment is required or failed, or we must “act now”; impersonating our boss or employer, important institutions like the bank, or a delivery service; or sending files or attachments that seem innocuous but install malware when opened.

Recognizing the tricks they may use makes it easier to pause and verify before reacting.

Practical checks

There are some easy things we can do to protect ourselves from potential cybersecurity incidents.

Hover over links to confirm the real destination; be on the lookout for misspellings, odd phrasing, slightly altered addresses or domains, unexpected requests for personal information or anything that causes a sense of urgency or immediacy; ensure the sender is real and contact them directly to verify; and treat all unsolicited attachments as unsafe unless we are 100% certain about the sender.

Notice

Our Local Agency must contact the State WIC Office within 24 hours of discovering a cybersecurity incident.

The initial notification must include our agency name and ID, the date and time we discovered the incident, the type of incident (such as malware, phishing, unauthorized access, etc.), potentially impacted systems or user accounts, whether participant data may be involved, and our local agency's response actions and immediate next steps.

Cooperate

We must cooperate with the State WIC Office, MNIT, and local IT staff during investigation, containment, and remediation activities following a cybersecurity incident.

Documentation

After remediation of the cybersecurity incident, our local agency must retain documentation for 6 years that includes a summary of the incident and root cause (if determined), actions taken to contain and remediate the incident, any user account resets, device reimaging, or system restoration performed, and correction actions taken to prevent recurrence.

This documentation must be provided to the State WIC Office for review upon request.

References

The following were referenced in this module.

Click the button to continue.

- 1.7 Data Privacy (https://www.health.state.mn.us/docs/people/wic/localagency/program/mom/chsctns/ch1/sctn1_7.pdf)
- 1.8 Data Sharing (https://www.health.state.mn.us/docs/people/wic/localagency/program/mom/chsctns/ch1/sctn1_8.pdf)
- 9.4: Network, Browser, and User Access Security (https://www.health.state.mn.us/docs/people/wic/localagency/program/mom/chsctns/ch9/sctn9_4.pdf)
- Participant Data Confidentiality (https://www.health.state.mn.us/docs/people/wic/localagency/dataprivacy.pdf)

Continue 1

Next, take a few minutes to see what we've learned in the Security Training Review 1 module.

Continue 2

We'll continue our security review for all WIC Program staff in the Security Training 2 module where we'll look at Physical and System Security.

End Slide

Thank you for reviewing the Security training 1 module provided by the MN Department of Health WIC Program.

Revisions

March 2026 – Added information about cybersecurity incidents (MOM 9.4).

August 2025 – Added information about data privacy and data sharing (split module into 4).

October 2020 – updated information and policies.

*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.*