Security Training Review 1 – What do you know now?

SCRIPT - REVISED MARCH 2026

Introduction

Welcome to the Security Training Review 1 module for all WIC Program staff provided by the Minnesota Department of Health WIC Program.

The purpose of this module is to see what you know now that you've reviewed the Security Training 1 module.

Overview

This module has at least one true/false or multiple choice question for the following topics: data privacy, sharing WIC data, data breaches, and cybersecurity incidents.

If you prefer to read the questions and answers yourself, feel free to mute the audio.

There is no requirement for how many questions you answer correctly.

Set a goal, 100% maybe, and see how you do.

Data privacy

Review Question 1

What do you know **now**? True or false.

Because participation in WIC is voluntary, the information participants provide is not confidential.

Answer 1

The answer is false.

WIC participation is voluntary but in order for us to do a full assessment of eligibility and referral needs, we require our participants to divulge private and confidential information to us.

Because of this, federal regulations require that we always ensure strict confidentiality of WIC data.

Review Question 2

What do you know **now**? Multiple choice (select one).

Which of the following is **not** considered private or confidential information?

A) Information that **relates to** a family member of an applicant or participant.

B) Names and contact information.

C) Health data.

D) Appointment information.

E) None. All of these are private and confidential.

Answer 2

The answer is: E.

All of the following are considered private and confidential (E).

Any information that can be used to identify an individual person or relates to an applicant, participant, or family member(s) (A) is private and confidential.

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

Sharing WIC data

Review question 3

What do you know **now**? True or false.

We can include release forms to request health information as part of the application and/or certification process.

Answer 3

The answer is **true**.

Release forms that authorize the program to request specific health information from health care providers, such as measurements, bloodwork, or medical formula needs, can be included as part of the initial application or prior to completing a certification.

This is an exception. All other release of information forms should be completed after application and certification.

Review Question 4

What do you know **now**? Multiple choice (select one).

Which is **not** true about Release of Information (ROI) forms?

A) Must be signed by an individual with legal authority to consent.

B) Generally, must be obtained after the application and certification process is complete.

C) Participants can be required to sign.

D) Should primarily be used for continuity of care and for the participant's benefit.

E) None. All of these are true.

Answer 4

The answer is: C.

General Release of Information (ROI) forms should primarily be used for continuity of care and for the participant's benefit (D).

Requiring they be completed after application or certification (B) ensures there isn't any implied pressure or undue influence for the individual with legal authority to consent to sign (A) because we cannot require a signature (C).

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

Review question 5

What do you know **now**? True or false.

If local authorities suspect, or are investigating, a third-party report of child abuse or neglect and request WIC data, we must provide the requested information since we are mandated reporters for abuse.

Answer 5

The answer is: false.

We cannot disclose WIC data without either a court order or warrant explicitly granting access to specific WIC data in cases where abuse has been reported outside of WIC. A subpoena is generally not adequate.

Otherwise, we must have a release of information signed by an authorized individual to provide any information to requesting authorities.

If **we suspect or identify** child abuse or neglect, we may provide information to the proper authorities without first obtaining written consent.

Data breaches

Review question 6

What do you know **now**? True or false.

A data breach has occurred if we accidentally disclose private data.

Answer 6

The answer is: true.

Whether unintentional or not, any disclosure of private data is considered a data breach.

Review question 7

What do you know **now**? Multiple choice. Select all that apply.

Which of the following examples would be considered a potential data breach?

A) Leaving the search page, with search results, on our computer while we run to the bathroom.

B) Leaving a report with authorized representative's names on it on our desk overnight.

C) Sharing a report that has the Household ID and State WIC ID on it.

D) Addressing WIC-specific mail to an incorrect mail address.

E) Losing our agency-issued phone.

Answer 7

The answers are: A, B, D, and E.

Anytime we leave data exposed to be viewed by unknown persons, we are risking a data breach. This would include walking away from our computer when it is displaying participant information (A), leaving documents or reports with any information about, or **related to**, an applicant or participant (B) exposed, inadvertently sharing a person is on WIC by sending WIC mail to the wrong address (D), as well as losing by misplacement or theft any technological hardware (E).

The Household ID and State WIC ID (C) are both unique non-private identifiers and are not considered personally identifiable information.

Review question 8

What do you know **now**? True or false.

If a data breach occurs, or is thought to have occurred, we should inform our WIC coordinator/supervisor, the state WIC MIS & Data and WIC Nutrition & Clinic supervisors, and our state WIC consultant.

Answer 8

The answer is: true.

We must inform our WIC coordinator/supervisor and the state office, including the MIS & Data supervisor, Nutrition Services supervisor, and our state WIC consultant if we think, or know, a data breach has occurred.

Review question 9

What do you know **now**? Multiple choice. Select one.

What information don't we have to provide if a data breach may have occurred?

A) Our agency name and ID.

B) List of missing equipment or disclosed participant data.

C) Location, date and time, and circumstances.

D) Copy of the police report (if applicable).

E) We have to provide all of these.

Answer 9

The answer is: E.

If a data breach has occurred, or is even thought to have occurred, we must provide our agency name and ID (A), a list of missing equipment or what participant data was disclosed (B), location, date, time and circumstances of the breach (C), and a copy of the police report (if applicable) (D).

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

Cybersecurity incidents

Review question 10

What do you know **now**? True or false.

An example of a cybersecurity incident would be if a WIC staff person were to access our Information System after being fired.

Answer 10

The answer is: true.

Cybersecurity incidents include unauthorized access to system or user accounts (as well as malware, ransomware, phishing, network intrusions, security breaches, and any cyber incident that may expose private participant data).

Review question 11

What do you know **now**? Multiple choice. Select the correct answer.

We receive an email message from our supervisor with the subject of "URGENT: Please verify list ASAP!" and a file we don't recognize. What should we do?

A) Open the file and respond immediately since our supervisor sent it.

B) Save the file to another location on our computer then open it.

C) Examine the email carefully for odd phrasing or misspelled words then call our supervisor to confirm she sent the email and verify what the file is.

D) Reply to the email to confirm its authenticity.

E) Forward the email to a coworker to get their opinion about it.

Answer 11

The answer is: C.

We have all the power in controlling whether we are impacted by malicious intentions. Slow down, treat every email as potentially suspicious and unsolicited attachments or unknown links as unsafe, and always verify the sender if an email is received that is unexpected or creates a sense of urgency or fear.

References

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)
- 9.3 Information System Software (https://www.health.state.mn.us/docs/people/wic/localagency/program/mom/chsctns/ch9/sctn9_3.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)
- 9.6 Electronic Communications Security (https://www.health.state.mn.us/docs/people/wic/localagency/program/mom/chsctns/ch9/sctn9_6.pdf)

- Participant Data Confidentiality (https://www.health.state.mn.us/docs/people/wic/localagency/dataprivacy.pdf)

End slides

Thank you

How'd you do?

Continue your annual security training with Module 2: Physical and System Security.

End Slide

Thank you for reviewing this security review module provided by the Minnesota Department of Health WIC Program.

Revisions

March 2026 – separated review module into 3 based on contents of training modules; added questions re: cybersecurity incidents.

August 2025 – updated for WINNIE information system.

*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.