Security Training Review 3 – What do you know now?

SCRIPT - REVISED AUGUST 2025

Introduction

Welcome to the Security Training Review 3 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 3 module.

Overview

This module has at least one true/false, multiple-choice, or fill-in-text question for each of the following topics: browser security, network security, data storage, electronic communications, and secure sites.

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.

Browser security

Review question 1

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

We are putting both ourselves and our participants' private data at risk if we have our browser save our username and password.

Answer 1

The answer is: true.

Auto-saving our username and password puts both us and our participants' data at risk.

Since anyone using our computer, authorized or not, can automatically login to our information system using our saved credentials, we are at risk of someone committing fraudulent actions under our name as well as allowing unauthorized access to all the confidential data contained in our database.

Network security

Review question 2

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

Which of the following indicate a security protocol is being used when we connect to an unknown wireless network?

A) Agree to legal terms.

B) Register an account.

C) Make sure there is an “s” in the https:// in a URL.

D) Enter a password.

E) Look for a sign indicating secure wi-fi is available.

Answer 2

The answers are: A, B, and D.

Before connecting to a wireless network, we should be required to do at least one of the following: agree to legal terms (A), register an account (B) , or enter a password (D), all of which indicate a security protocol is being used.

The “s” in https:// indicates the connection between a browser and a website is secure and encrypted (C), but doesn’t tell us if the network is secure and a sign (E)? Well, that’s just words. When connecting, the wireless network must require us to do something to ensure it’s secure.

Review question 3

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

When working remotely, a Virtual Private Network (VPN) should be used whenever possible since it creates a secure and private connection over the internet.

Answer 3

The answer is: true.

VPNs provide a “tunnel” that protects us by creating a secure and private connection as we send data over the internet.

It handles encryption and routing and ensures that our data stays secure from login to logout.

Data Storage

Review question 4

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

All downloaded documents must be deleted from our Downloads folder and Recycle Bin at least once a week.

Answer 4

The answer is: false.

Whether our agency has a scheduled task that does it automatically or we do it manually, all downloaded documents with private data must be deleted every day from our Downloads folder and Recycle Bin.

Review question 5

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

Which of the following statements is **true**?

A) Proofs submitted electronically should be scanned into the participant folder before deleting.

B) Flash/thumb drives should not be used to store private information since they are not secure.

C) It is OK to save documents with private data to a Share drive as long as it belongs to Public Health.

D) We shouldn't delete documents submitted electronically; we must keep them per our data retention schedule.

E) None of these are true.

Answer 5

The answer is: B.

Removable storage devices can be easily lost or misplaced, and "deleted" information is used as space to be overwritten (not deleted), which is why their use is strongly discouraged (meaning: we shouldn't use them (B)).

In general, electronic proofs and documents should be deleted (D) once reviewed, used for WIC services, or processed and not scanned or imported (A) (unless policy requires it). They also should not be saved to a share drive unless we can ensure only those who should have access to private WIC data have access to the drive (C).

Electronic communications

Review question 6

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

Email communications are usually considered secure, and we can assume our email is encrypted since we work for a public health program.

Answer 6

The answer is: false.

We cannot assume our email communications are safe for private information. We should contact our county IT to find out if it's secure and if not, how we could send a secure email if needed.

Review question 7

What do you know **now**? Enter the answer into the text field (not case-sensitive) and click the Submit button.

Use the non-private _____ to refer to participants in email. This is all we need to identify a participant.

Answer 7

The answer is: State WIC ID

The State WIC ID is a unique, non-private, individual identifier, and is all we need to use to reference a specific participant.

Avoid using participant names, which are private and confidential.

Review question 8

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

It is OK to email a participant using our personal Gmail account as long as we've obtained consent from the participant to email them.

Answer 8

The answer is: false.

We should always use our agency email if emailing participants; we should never use our personal email.

Review question 9

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

We can save participant names to our agency-issued phone's contact list, but never our personal phones.

Answer 9

The answer is: false.

We should never save participant names or contact information to any phone contact lists regardless of whether personal or agency-issued.

Review question 10

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

Before a participant first uses Contact Us they must opt in for texting, but this only applies to Mobile Management. To use another texting platform, we must obtain and document consent.

Answer 10

The answer is: true.

When a participant opts in for texting on their app, it only provides texting consent within Mobile Management. An additional release must be acquired and documented to text using another platform.

Review question 11

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

As long as we are using the text thread started in Mobile Management, it is OK to send a text back asking the participant to send a clearer image of their driver's license.

Answer 11

The answer is: false.

Texting is not a secure form of communication.

Only the Contact Us transmission is secure. When using Mobile Management, we should never ask participants to text us back on the same texting thread with personal information. If there is any texting back-and-forth, no personal information should ever be texted by us or the participants.

If they need to resubmit an image, we should always ask them to start a new Contact Us message to ensure the image is transmitted securely.

Review question 12

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

What are some of the requirements when using text messages?

A) Provide the opportunity to opt in or out when using a texting platform.

B) Obtain a verbal consent (which is all that is needed as long as it is documented in a local use field).

C) Obtain written consent before texting when using the Mobile Management Portal.

D) Scan or import written release of information into participant folders in the information system.

E) Inform participant that texting is not secure if they want to text personal information.

Answer 12

The answers are: A, D, and E.

If we have a texting platform, it must be optional with the right to opt in or out (A). We can obtain **temporary** verbal consent and document it in a local use field (B) but must obtain a written release of information (this is **not** needed when using the Mobile Management Portal because consent is given through the app (C)).

The written release of information must be scanned or imported into the appropriate participant folders in the information system (D).

If a participant wants to text personal information, we must inform them texting is not secure (E) and provide alternative methods for submitting the information.

Review question 13

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

Which of the following is not a secure alternative electronic submission method that we can offer to participants?

A) WIC App Contact Us >> Submit Documents feature.

B) MN WIC Participant Documents submission form.

C) Text or email to an agency-issued phone.

D) MN WIC Online Application form.

E) All of these are a secure alternative.

Answer 13

The answer is: C.

We should never use our personal or an agency-issued phone to text or email with participants (C).

Acceptable alternative methods for submitting documents securely include: the WIC app's Contact Us feature that submits to the Mobile Management Portal (A); the MN WIC

Participants Documents submission form (B); and the MN WIC Online Application form (D) (as well as secure or encrypted email).

Secure sites

Review question 14

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

Which of the following provide data that can **always** be shared with other people and programs?

A) MN Fact Sheets on the website.

B) Local Agency Portal.

C) Infoview.

D) Reports & Data page on the website.

E) FileZilla.

Answer 14

The answers are: A and D.

The key word is always.

The MN Fact Sheets (A) and reports on the MDH WIC Reports & Data page (D) on the website have aggregated, numeric, and summary WIC data that we can share with administrators and other interested people or programs.

The Local Agency Portal (B) has reports with small numbers and private data while Infoview (C) has ad-hoc reports that most often contain private data. FileZilla (E) is a secure location where we store and allow transfer of documents with private information. In general, or unless indicated otherwise, we shouldn't share content from these sites with others.

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)

Thank you

How'd you do?

Thank you! You have completed the annual WIC Program security training!

End Slide

<no audio>

Revisions

March 2026 – added questions re: email, environments, and 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.*