Security Training 3 – Access, Storage, Communications, and Sites with Data

SCRIPT - REVISED AUGUST 2025

Introduction

Welcome to the Security Training 3 module: Access, Storage, Communications and Sites with Data.

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

Overview 1

In this module, we'll take a look at browser security, network security, data storage, electronic communications, and secure sites with participant data.

Browser security

Knowledge check 1

What do you know?

The path between our information system and our computer is encrypted. We know this because of the "s" in "https" in its URL. True or False.

Https

Web services use HTTPS to create a secure, encrypted path between the information system servers and our computers.

Knowledge check 2

What do you know?

Since the information system requires multi-factor authentication (MFA), we can have the browser save our username and password. True or false.

Saving login on browser

If prompted by the browser, we should NEVER select to save our username and/or password to the browser.

Auto-saving our usernames and passwords is a huge security risk because anyone that uses our computer, authorized or unauthorized, can automatically login to our information system using our credentials, putting both ourselves and our participants' private data in jeopardy.

Network security

Knowledge check 3

What do you know?

Since wireless networks tend to be secure, we can use the network available at our local coffee shop to do WIC work as long as we can access their wi-fi. True or false.

Working remotely

When using a wireless network, it is recommended that a security protocol be used, which requires that we do one of the following before connecting to the network: agree to legal terms, register an account, or enter a password.

VPN

Whenever possible, we should use a Virtual Private Network (VPN) when working remotely.

VPN is a technology that creates a **secure and private connection** over the internet.

VPNs provide what can be thought of as a protective “tunnel” to handle the encryption and routing of our data, ensuring it stays secure from start to finish.

Data Storage

Knowledge check 4

What do you know?

Documents we download from a WIC information system can be stored in our Downloads folder as long as the folder is on our own work computer, which we don't share with anyone else. True or false.

Downloads

Documents that contain private data and are downloaded from the WIC information system, Mobile Management, other document submittal systems, or Infoview **must be deleted from our Downloads folder and Recycle Bin daily.**

Some local agencies have a scheduled task that deletes all files from the Downloads folder and Recycle Bin each time a user logs onto their computer and at 8 pm daily if the computer is not shut down overnight.

If our agency doesn't automatically delete our downloads, we are responsible for ensuring we delete any contents that contain private data from our Downloads folder and Recycle Bin every day.

More information about how to manage our downloads can be found under documents on the WINNIE Training page.

Electronic submissions

We should delete electronic submissions, such as proofs, online applications, messages, etc. as soon as they are reviewed, used for WIC services, and/or processed.

And unless required by MN WIC policy, we should not scan nor import these into the participant folder nor save them to our electronic devices, such as our computers/tablets/phones, etc.

Knowledge check 5

What do you know?

It is OK to use the Share drive used by our agency's public health programs' staff to store files with personal WIC data on them. True or false.

Share drives

Shared, or networked, drives are available to many of us for storing our documents at work.

However, if they are used by other staff within our agency who shouldn't have access to private or confidential WIC information, we cannot use that drive to store that type of information.

Always keep in mind when saving or storing information who should be allowed to have access to it and who actually does have, or will have, access.

Removable media

In general, the WIC state office strongly discourages using flash or thumb drives to store information that contains personal or private WIC data.

These kinds of storage devices are not considered secure.

They can be easily lost or misplaced and when information is "deleted", it is actually marked as available space to be overwritten, so…not deleted and can be restored or retrieved.

Electronic communications

Knowledge check 6

What do you know?

As long as we send an email directly to a WIC state office staff person, it is OK to attach a report output that includes participant names. True or false.

Email

Email is usually not considered a secure form of communication for private information.

In many cases, email may be encrypted, but with the multitude of different email providers, we cannot just assume our email is encrypted and secure.

There are methods for sending a secure email and we should contact our county IT to find out what may be available to us.

In general, though, we should never need to send a participant's name via email.

Use the State WIC ID instead, the participant's unique, non-private, individual identifier.

Knowledge check 7

What do you know?

Text messaging is **not** considered a secure form of communication. True or false.

Text messaging 1

Texting is not secure.

We must obtain consent before communicating via text, and we must provide the opportunity to opt in or out of text messaging (this applies to email communications as well).

An initial verbal temporary consent can be documented using a local use field in the information system, but we **must** get a written release of information signed by a person with the authority to consent at the next participant contact.

This must be scanned or imported into the appropriate participant folders in the information system.

Mobile Management texts

If our agency uses the Mobile Management portal, documented permission is not required.

The Contact Us feature that sends texts to Mobile Management requires the WIC App user to first opt-in to text messaging.

Text messaging 2

Personal information should **never** be requested or sent by text.

If a participant wants to submit personal information via text message, we **must** inform them that texting is not secure and offer alternate electronic submission methods, such as the WIC

App Contact Us >> Submit Documents feature, MN WIC Participants Documents submission Form, MN WIC Online Application or secure or encrypted email.

Secure sites

Knowledge check 8

What do you know?

The reports available to us on the Local Agency Portal were created so that we can share our WIC data with other people and programs. True or false.

Local Agency Portal

The Local Agency Portal is a secure SharePoint site that WIC staff with access must login to view.

It contains reports that include small numbers and private data.

Since individual participants could be identified, these data should not be shared with non-WIC persons.

Infoview

Infoview is another secure site that WIC staff with access must login to.

It provides ad-hoc reports, mostly containing private data.

Sharing and exporting of Infoview outputs must follow all policies pertaining to data sharing and ensuring the security of printed or downloaded documents.

Other data

Data that can be shared are available on the Reports & Data page of the MDH WIC website.

These are aggregate, numeric, and/or summary WIC data.

Individual WIC participants cannot be identified, and these data are considered public and may be used for a variety of purposes.

FileZilla

The FileZilla FTP site is a secure location the state uses to store and allow transfer of documents with private information.

Agencies are able to download these documents securely since they are encrypted during the transfer.

In summary

Summary

In summary, the primary take-away from these security training modules should be that we must always perform our WIC services with the utmost care when accessing, sharing, using, viewing, printing, downloading, transporting, storing, communicating, or providing confidential information to ensure that the information we've been entrusted with is always secure.

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)
- Documents on WINNIE Training page (https://www.health.state.mn.us/people/wic/localagency/winnie/training.html#documents)

Go to

Let's see what we've learned. Go to the Security Review training module to complete the security training.

End Slide

Thank you for reviewing this Security Training provided by the MN Department of Health WIC Program.

Revisions

August 2025 – updated information and policies for new browser-based information system.

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.*

This institution is an equal opportunity provider.