Security Training Review – What do you know now?

SCRIPT - REVISED AUGUST 2025

Introduction

Welcome to the Security Training Review 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 modules.

Overview

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

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.

Physical security

Review question 6

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

Which of the following statements are true about physical security?

A) CONTROL + L locks our computer.

B) A computer lock should be secured to a fixed, stationary object.

C) We should never leave our computer equipment in a car when traveling.

D) We should never send documents with private information to a personal or home printer.

E) Printed documents with private data should be recycled once were done reviewing/using them.

Answer 6

The answers are: B, C, and D.

Whenever we leave our computers, we should use Control + Alt + Delete or the Windows key + L (A) to lock our computers and if we have a physical lock, it should be secured to a fixed non-movable object (B).

When traveling, we should always keep our computer equipment with us and never leave it in the car, not even locked in the trunk (C).

As for printed documents with private information, they should **never** be sent to our personal or home printer (D) and once we are done with them, we should destroy them in the same way our agency destroys other confidential documents (E).

Review question 7

What do you know **now**? Enter 1 word into the text field (not case-sensitive) and click the Submit button.

Reports and documents with private data should always be stored in a secure place, such as a _____ drawer or file cabinet when not using or viewing them.

Answer 6

The answer is: locked

Documents must be secured just like access to our computer.

Leaving documents containing private data out for anyone to be able to view is neglecting our responsibility to our participants to protect their confidential information.

System security

Review question 8

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

Which of the following does **not** increase security?

A) Requiring full-disk encryption for all computers used for WIC.

B) Sharing our password with our supervisor in case they need to login to our computer.

C) Tracking system logins, logouts, and actions performed.

D) Limiting browser sessions to 30 minutes without a server call.

E) Requiring a certain level of password complexity.

Answer 8

The answer is: B.

Sharing our password? Never. It is private and should **never** be shared with **anyone** (B).

Requiring full-disk encryption (A), tracking our use of the information system (C), limiting inactive browser sessions (D), and ensuring our password meet basic requirements (E) are all ways that we increase security.

Review question 9

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

What are some of the common pitfalls we should avoid when creating our passwords?

A) Using a passphrase that is easier to remember.

B) Using correctly spelled words.

C) Using names or pet names.

D) Using the first letters of words in a title, song, or poem.

E) Using celebratory dates, personal information, or favorites.

Answer 9

The answers are: B, C, and E.

Some of the common pitfalls when creating passwords include using correctly spelled words (B), names or pet names (C), keyboard sequences, personal info, celebratory dates (birthday, anniversary, etc.), favorite teams, numbers, and movies (E).

Using a passphrase (A) or the first letters of words in a title, song, or poem (D) are methods that use mnemonics to help us create and remember complex passwords.

Review question 10

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

We should use the Remember Me toggle on the Multi-factor Authentication (MFA) page so that when our co-worker logs into our computer at lunch, she won't have to enter the MFA code.

Answer 10

The answer is: false**.**

The Remember Me toggle on the MFA page allows us to bypass the MFA process if we have to login more than once on a specific day (this "bypass" expires at midnight).

However, if we share our computer with others, we should not toggle on Remember Me. **We are all required to get the MFA the first time we login each day.**

Review question 11

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

Which of the following statements about deactivations is true?

A) Deactivation puts access on hold in case a staff person returns to WIC after leaving.

B) Deactivation is not a security measure.

C) We should deactivate users with planned absences lasting one week or longer.

D) Our Coordinator must call the MN Help Desk immediately if a staff person quits without notice.

E) We should submit a form and provide a date to deactivate our username if we decide to leave WIC.

Answer 11

The answer is: D.

Our coordinator should call the Help Desk to immediately deactivate a username if the person leaves WIC unexpectedly (D) since deactivation is a security measure (B) that safeguards the system by removing access (A).

Our coordinator should also submit a form when staff leave WIC to deactivate the username (E) and should request a "hold" be put on a username if a planned absence is going to last 4 weeks or more (C).

Browser security

Review question 12

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 12

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 13

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 13

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 14

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 14

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 15

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 15

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 16

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 16

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 17

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 17

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 18

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 18

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 19

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 19

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 20

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 20

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 21

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 21

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.

Data breaches

Review question 22

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

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

Answer 22

The answer is: true.

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

Review question 23

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 23

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 24

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 24

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 25

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 25

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.

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)

Thank you

How'd you do?

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

Click the button to continue.

End Slide

<no audio>

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.