Security Training Module Script

REVISED OCTOBER 2020

Introduction

Welcome to the Security Training Module for all MN WIC Program staff provided by the MN Department of Health WIC Program.

Overview

The purpose of this training is to review the processes for ensuring "the security of the WIC Information System networks, data and computer equipment". (Ref: MOM, Section 9.3)

Expectations

In order to do this, we must understand and recognize what the expectations are for maintaining participant privacy and data confidentiality;

and what our responsibilities are towards ensuring that we protect ourselves and our participants from security breaches.

Identify

During this training, we will help identify the security procedures that we can use to protect our computer equipment, along with the system's security features that help us to protect ourselves and our participants' data.

Lastly, we'll discuss what to do when a security incident occurs.

Data Privacy

Question #1

What do you know?

WIC data is private under Federal WIC Regulation. True or False.

Private Data

"WIC data is private under Federal WIC Regulations, Section 246.2(d). This regulation restricts the use and disclosure of information from WIC applicants and participants to persons directly connected with the administration or enforcement of the program..." (Ref. MOM, Section 1.7)

Responsibilities

It is our responsibility, as representatives of the WIC Program, to secure access to participant's private information and "ensure the security of WIC Information System networks, data and computer equipment". (Ref: MOM, Section 9.3)

System Security Features

Question #2

What do you know?

My Windows login is a system security feature. True or False.

Window's Login

Although our login "unlocks" the computer so that we can use it, which is probably the security reason we are most familiar with, it also functions as a key to unlock the encrypted information on our computer.

Encryption

Our desktops and laptops have something called "full-disk encryption".

This is technology that protects information on the computer by converting it into a non-readable format, making it unreadable or unusable by anyone that does not have the key to unlock it.

Key

Our Windows password is the key to unlocking the encryption on our hard drive so that we can access, read and use the information stored on our computer.

Question #3

What do you know?

The "s" in "https://" in the URL means the path between the site and my computer is encrypted. True or False.

https

The "s" in the https:// in a URL indicates that it is secure.

Web service uses HTTPS to create a secure, encrypted path between the servers and our computers.

Question #4

What do you know?

Wireless connections aren't secure. True or False.

Wireless

Wireless connections can be just as secure if using a properly configured and password-protected wireless connection.

Risk occurs when the source of the wireless connection is unknown or isn't password protected.

The wireless network must require a password to be secure. Never use a wireless network that isn't password-protected.

Teleworking

When working remotely, while our home network may be secure, the additional use of VPN is preferable because it protects the transmitted data with an additional layer of security.

However, VPN is not required for teleworking.

Question #5

What do you know?

You are required to log into the WIC Information System… Multiple Choice.

A – To make your job harder

B – As another security measure

C – To protect data in the Information System from unauthorized users

D – To protect ourselves from others performing actions we could be held responsible for

E – Answers B, C and D

Logging In

Logging into the Information System with our unique username and individual passwords is another security measure that protects information from unauthorized users and ourselves from others performing actions on our computers for which we could be held responsible.

Always Login

We must always make sure to login before making any changes in the WIC Information System.

By logging in, we are telling the system, and any system or program auditors, who is responsible for the actions performed on that computer.

Keep Passwords Secret!

That is why it is so important that we don't share our passwords.

If anyone else were to learn our password, they could perform inappropriate actions, such as issuance fraud, that we could be held responsible for.

IS Tracking

The Information System has built-in functionality to track each user and the changes made by a user.

It creates logs to record activities such as when each user logs in, their session duration, and when the user logs out, as well as the ID of the workstation used.

This kind of oversight allows system and program auditors to ensure the integrity of the Information System and that it isn't being used inappropriately.

Passwords

Question #6

What do you know?

How often does your WIC Information System password expire? Multiple Choice.

A – Every 30 days

B – Every 60 days

C – Every 90 days

D – It doesn't. I need to remember to change it.

E – It doesn't. I never have to change it.

Expire

Our password for the WIC Information system expires every 90 days.

Standards

The Information System requires the following when creating a password: 8-16 characters, including upper and lower case letters, a number, and a special characters or symbol. It must also be different from the last 9 passwords we've used.

Creating PWs

When creating a new password, we should always try to make them hard for others to guess but easy for us to remember.

Using a passphrase can help us do just that.

Passphrase

A passphrase is creating a password from an easy to remember phrase, such as “candy is my happy”.

Run the words together, add some capitals, swap out symbols and numbers for a couple of letters, and we’ve made a really strong password: C@ndY1$MYh@99y

Change it

If you think your password has been compromised, be sure to change it immediately.

Remember, your password protects **you**!

Roles & Features

Question #7

What do you know?

WIC users are assigned a role, or roles, which limits a user’s access to certain modules or functions within the Information System. True or False.

User Access

All users have specific access to both locations and functions in the WIC Information System.

Users can only work in certain agencies and clinics, which they have been given rights to access, and can only perform functions allowed based on the role they’ve been assigned.

Roles

Role 1 – CPA can make any changes in the participant folder, and perform any function necessary for certification and issuance.

Role 2 – CPA w/Build Calendar is the same as Role 1 but with the added ability to build the appointment scheduling calendar.

Role 3 – View Only can only view the participant folder and cannot make any changes

Roles 1

Role 4 – Peer is for peer breastfeeding staff and limits their functions to notes, alerts, breastfeeding contacts, updating demographics and adding referrals. They can also view some parts of the participant folder.

Role 10 – LSA allows user to maintain referrals, medical clinics and providers and local use questions.

Role 11 – Clerk limits users to notes, alerts, updating demographics and ht/wt/blood, printing participant summary and VOC documents and scheduling appointments.

Features

Each specific and individual function in the system is considered a “feature” and each role is assigned an access level of none, view, add or full for that feature.

Feature 1

In this way, roles increase the system’s security by limiting access to only those functions we need in order to do our job.

User Deactivations

Question #8

What do you know?

If a user leaves unexpectedly, the agency's Coordinator should submit a WIC Information System User Request Form to deactivate the account as soon as possible. True or False.

Section 9.3

According to MOM policy (section 9.3), "in case of unplanned departure of staff, Local Agency Coordinators must call the Help Desk to immediately deactivate the user name account."

This is to safeguard against potential malicious activities that could be performed in the Information System to corrupt data, etc.

Planned

For users who will no longer be working for WIC on a pre-determined date, the Coordinator should submit a WIC Information System User Request Form to inform the State of the user’s departure date at least 3-5 days before that date.

Physical Security

Common Sense

Physical security is probably the easiest security measure to perform and also one of the easiest to neglect. It is often a matter of practicing common sense.

Question #9

What do you know?

Only laptops (not desktop computers) need to be secured to a stationary object using a Kensington lock. True or False.

Kensington Locks

Kensington locks should always be used to secure both our laptops and desktop computers to a stationary object.

This type of lock connects to the computer in such a way that it damages the hard drive, and renders the computer unusable and its information inaccessible, if forcibly removed.

Keys

Each lock comes with two keys.

For desktops, both keys, and for laptops, one key, should be stored in a secure location separate from where the computer is being used.

The second laptop key, which we use to lock our laptop and allows us to travel with it, should be kept on our person; not stored in a desk drawer or bag, where it might easily be found and used to unlock our computer.

Question #10

What do you know?

As long as your laptop is in a computer bag, it is always OK to leave it on the floor or backseat when traveling with it. True or False.

Traveling

Best practice, when traveling with our computers, is to lock the computer in the trunk.

This way, if we were to need to leave it in the car, such as if running errands between work and home…**never overnight**…it will be safe. It should never be left sitting out in the open, even if in a laptop bag, if we aren't in the car with it.

Physical Security & Data Privacy

Data Protectors

In WIC, one of our most important roles is data protector. It is our responsibility to safeguard private data that is entrusted to us as part of our daily work in the WIC Program.

Question #11

What do you know?

Using Ctrl + Alt + Del to lock your computer is one way to protect data privacy. True or False.

Lock Computer

Locking our computer before walking away from it, or leaving it unattended, is one of the simplest ways to protect our participants' data.

The fact that a person is on the WIC Program is private and any data on the WIC Information System's screens are private.

We can easily lock our computers using Ctrl + Alt + Del or pressing the Windows key and the letter "L".

When the computer is locked, only the person currently logged in (or a person with admin rights) can access the computer.

Our computers also auto-lock after 10 minutes of inactivity, which is another security safeguard.

Lock Computers 1

Since we never know who may walk by our computer, whether it is a member of our family, a friend, co-worker from a different department, or another participant, none of whom is privy to information that may be displayed on our WIC screens, leaving our computer unlocked and screens exposed so that they can be viewed by anyone walking by is neglecting our responsibility as data protectors.

Question #12

What do you know?

Printed materials with private data on them should be stored as securely as our computers. True or False.

Printed Materials

Printing information that contains private data is sometimes necessary and unavoidable, and it should be kept as securely as our computers.

Printed Materials 1

Reports, or other documents with private data, should not be left out in the open.

When printing to a shared printer, we should pick it up immediately after printing, and never allow it to sit on the printer where any person passing by might see it or accidentally pick it up.

Printed Materials 2

Printed materials with private data should be stored in a secure place, such as a lockable drawer or file cabinet, when not using them.

If the document is no longer being used it should be destroyed as appropriate; disposing of it in the same manner as our agency disposes of other private data.

Data Storage

Question #13

What do you know?

When you delete information from a flash drive, or from our computer, it is gone forever. True or False.

Removable Media

Information that has been deleted from flash drives or computers is not gone forever. It can always be restored or retrieved unless a "data wiping" process has occurred or the storage media has been physically destroyed.

Flash Drives

Flash, or thumb, drives are a means of data storage that is appropriate only for short-term use.

If any participant information has been saved to it, such as print screens or reports, it should be protected as diligently as our computers or printed documents. This means, when we aren't actively using it, the removable media device should be stored in a locked location, such as our desk or file cabinet.

Deleting Flash

We should always remove, or delete, private information stored on the removable media once it is no longer needed.

However, once any private data has been saved to a removable media device, even once deleted, we must still treat that device as if it still contains private information.

Remember, we can only assume information is no longer available on the device only once it has been destroyed. Even though it may look like the information is gone, it can still be easily recovered.

Share Drives

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

If the share drive is used by other staff within our agency who shouldn't have access to WIC private data, the share drive shouldn't be used to save WIC data.

Share Drives 1

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

Electronic Communication

Question #14

What do you know?

It is OK to send email with participant names because email is always secure and encrypted. True or False.

Email

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 determine what method may be available to us.

Emailing PPT Info

In general, there is never any reason to send a participant's name via email.

The purpose of the State WIC ID and Household ID is to provide a non-private unique identifier for a participant or their household and these IDs should always be used instead of a name.

FileZilla

The FileZilla FTP site is a secure location for storing and transferring documents.

The State uses the agencygateway to post documents or reports containing private data.

When a document is downloaded, it is encrypted during the transfer.

Social Engineering

Question #15

What do you know?

You should never automatically provide personal participant information when requested by email, phone or in person. True or False.

Requests

We should never automatically provide personal information after receiving a request regardless of whether via email, phone or in-person.

We must always verify that the requestor has been authorized to have access to this information and only disclose the information once we are 100% certain.

Requests 1

Remember, WIC Federal Regulation, "restricts the use and disclosure of information from WIC applicants and participants to persons directly connected with the administration or enforcement of the program…"

Best practice is to inform our supervisor or coordinator, and if necessary our State Consultant, when we receive these types of request.

Lost or Stolen Equipment

Question #16

What do you know?

If a computer with participant information is lost or stolen, Local Agencies must IMMEDIATELY contact the State WIC Program. True or False.

Lost/Stolen

Even though our computers are encrypted, if lost or stolen, there is still huge potential for compromising private participant information. It is taken very seriously at the State and needs to be taken just as seriously by each agency and WIC staff person.

Notify

It is paramount that we immediately contact the supervisor/coordinator of our WIC Program and the State Office, including the WIC MIS & Data Unit's Supervisor, the Nutrition & Clinic Unit's Supervisor and our agency's State Consultant.

We must provide the following information: our agency's name and ID number, a list of the missing equipment, the location, date/time and circumstances surrounding the loss or theft, and a copy of the police report if one was filed.

Repercussions

The repercussions of losing private data cannot be exaggerated and can be far-reaching. If data is lost, we may be required to notify our participants that their private information, however unintentionally, may now be in the hands of persons unknown.

Summary

The primary take-away from this training module should be that we must always take the utmost care when accessing, using, viewing, printing, transporting, storing, or providing private information to ensure that the information we've been entrusted with is always secure.

Go To

To see what you've learned by watching this module, please go to the Security Review Questions 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.

Minnesota Department of Health - WIC Program 85 E 7th Place, PO BOX 64882, ST PAUL MN 55164-0882; 651-201-4444, health.wic@state.mn.us, www.health.state.mn.us; To obtain this information in a different format, call: 651-201-4444