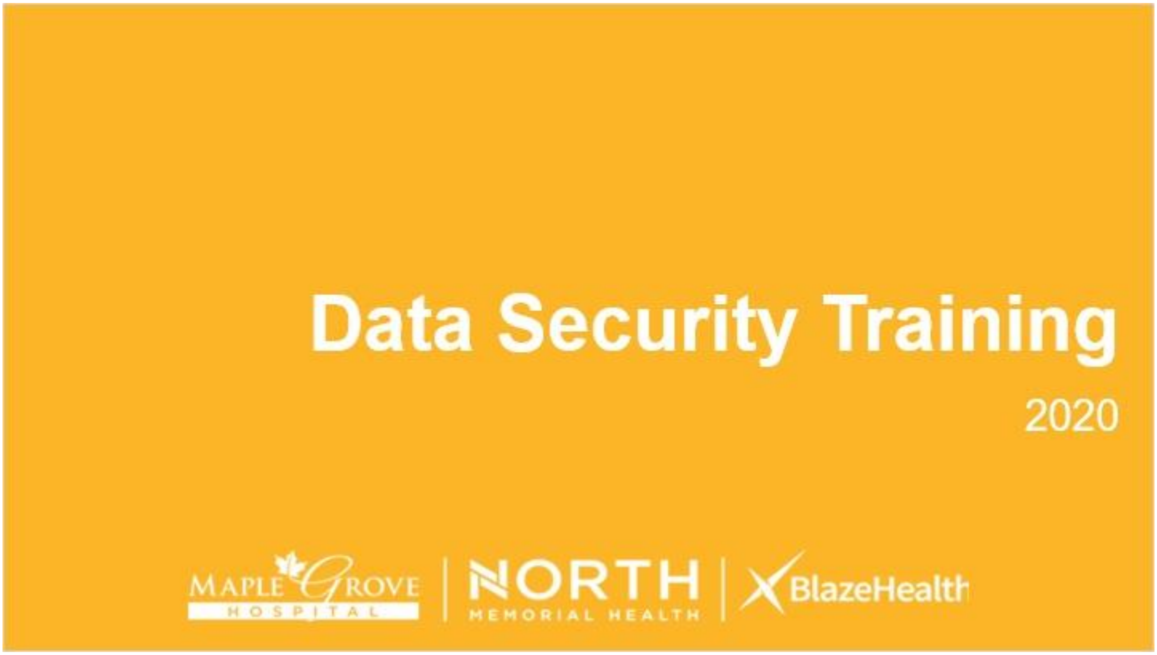
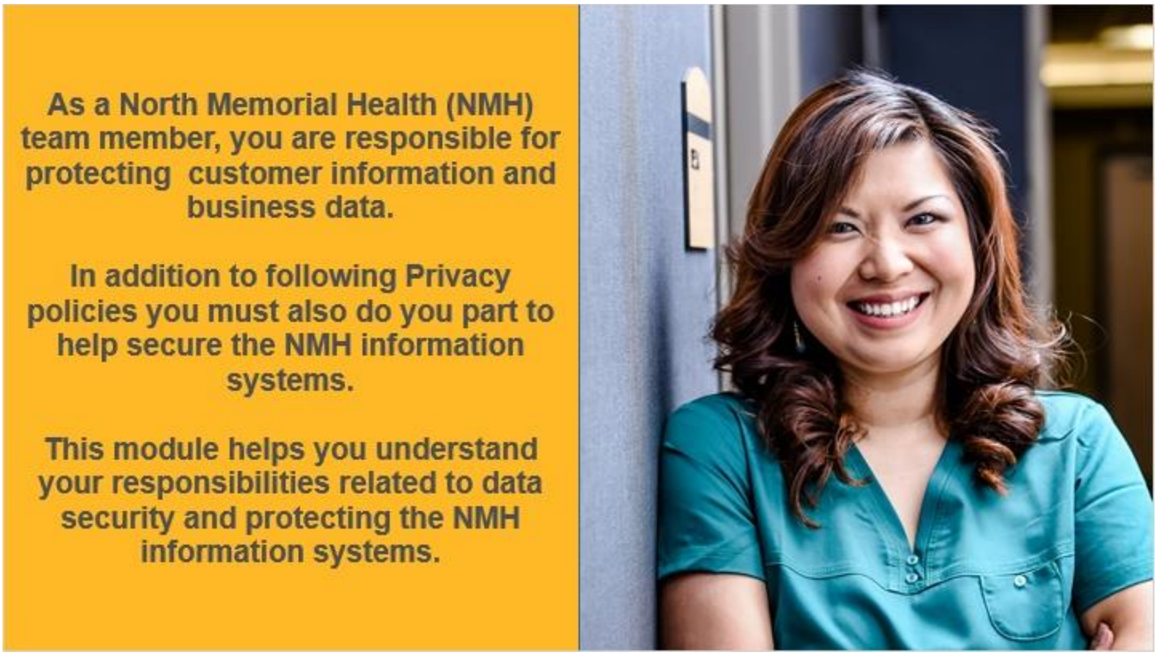
Data Security 2020



Data Security Training

2020

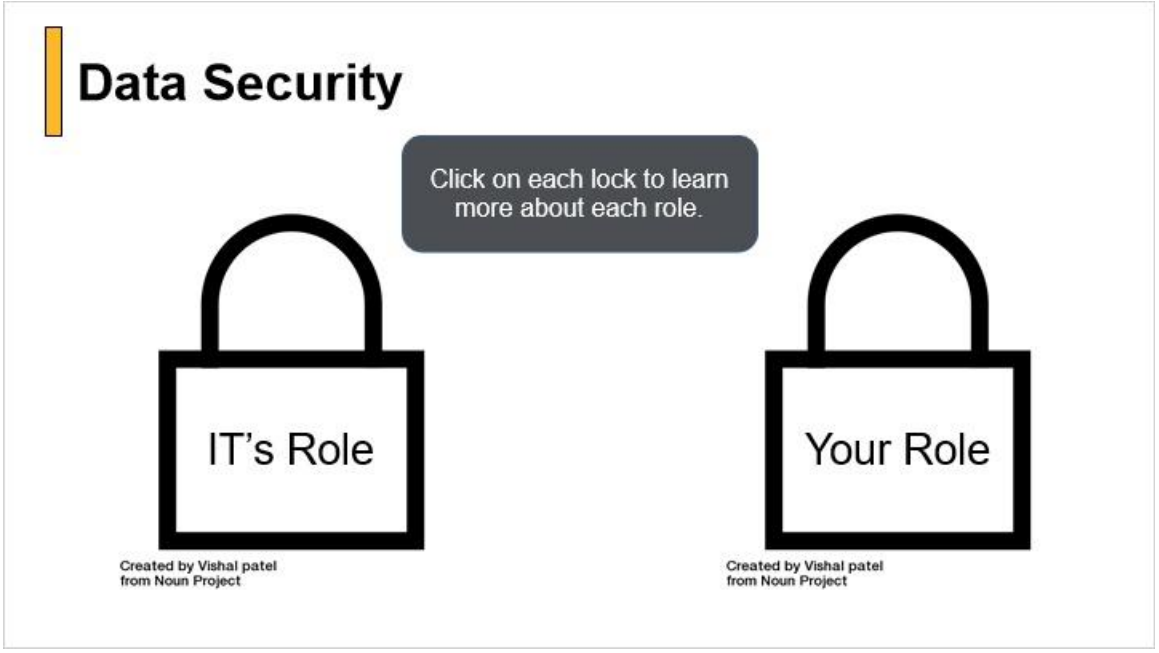
MAPLE GROVE HOSPITAL
NORTH MEMORIAL HEALTH
BlazeHealth



As a North Memorial Health (NMH) team member, you are responsible for protecting customer information and business data.

In addition to following Privacy policies you must also do you part to help secure the NMH information systems.

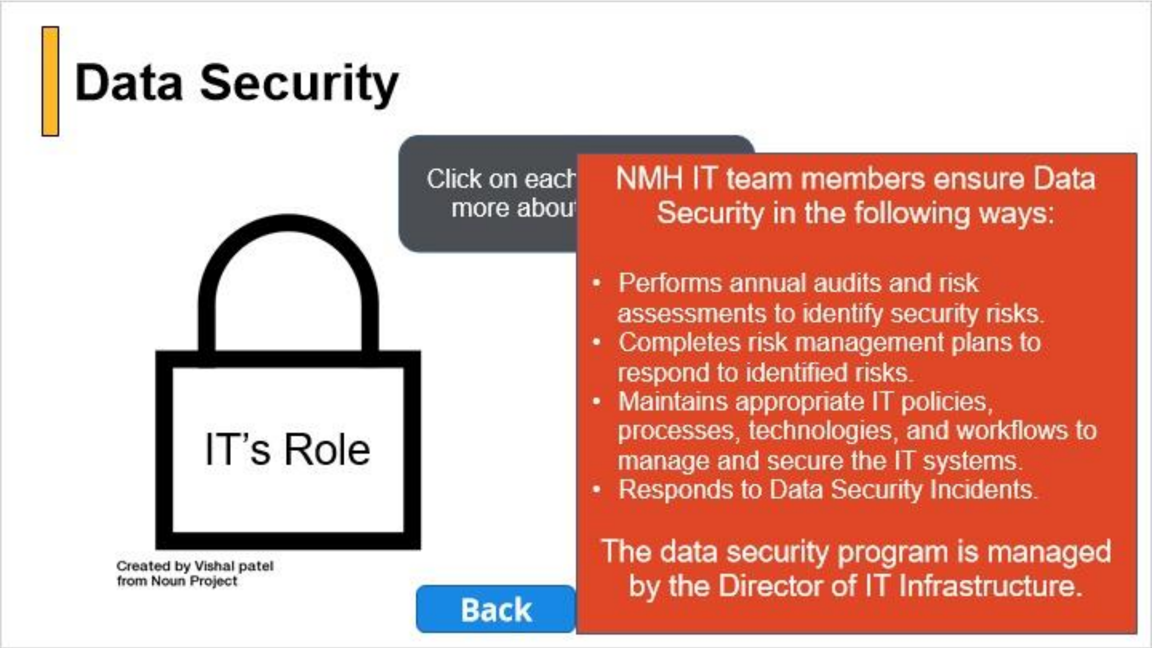
This module helps you understand your responsibilities related to data security and protecting the NMH information systems.



Data Security

Click on each lock to learn more about each role.

IT's Role
Your Role
Created by Vishal patel from Noun Project
Created by Vishal patel from Noun Project



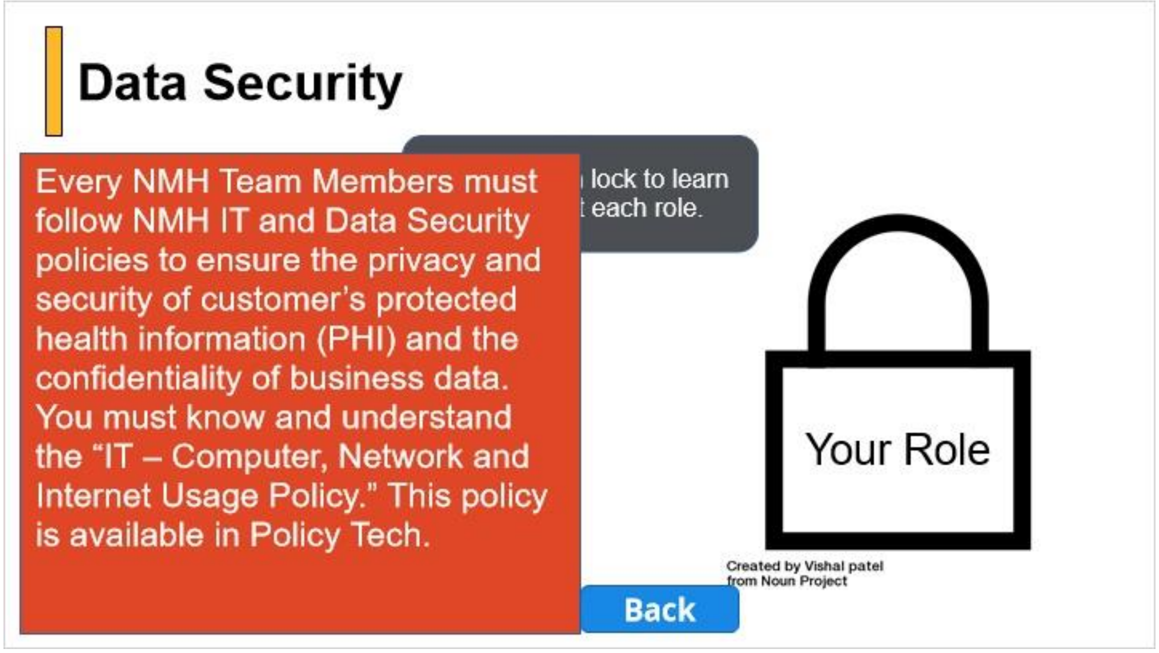
Data Security

Click on each
more abou

NMH IT team members ensure Data Security in the following ways:

- Performs annual audits and risk assessments to identify security risks.
- Completes risk management plans to respond to identified risks.
- Maintains appropriate IT policies, processes, technologies, and workflows to manage and secure the IT systems.
- Responds to Data Security Incidents.

The data security program is managed by the Director of IT Infrastructure.

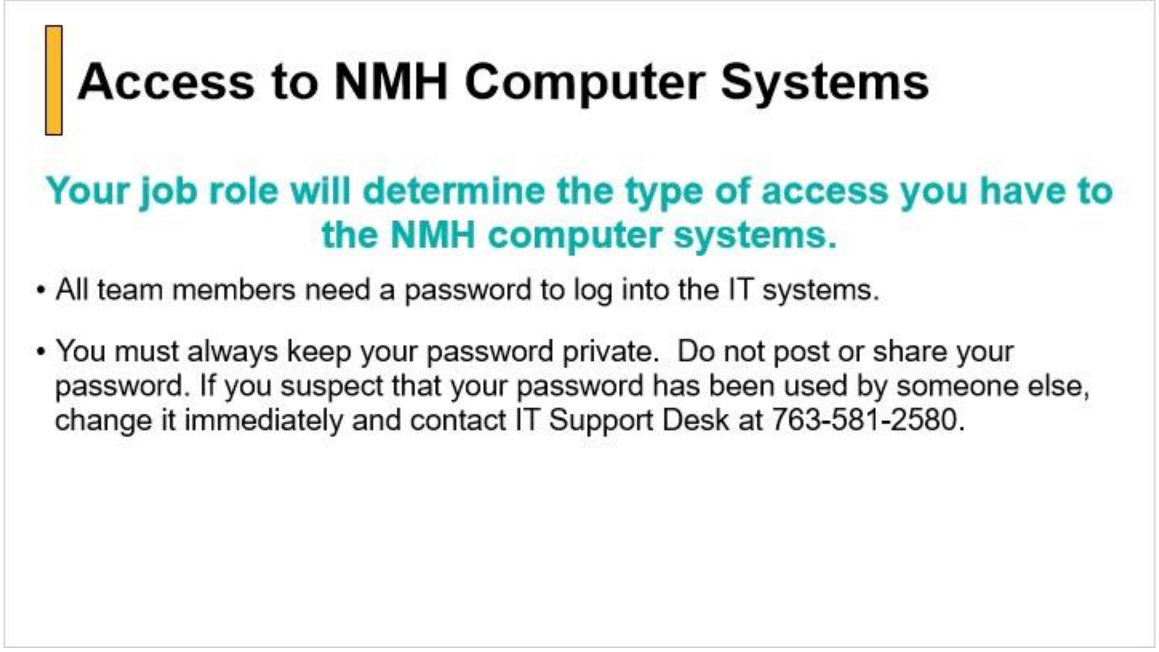


Data Security

Every NMH Team Members must follow NMH IT and Data Security policies to ensure the privacy and security of customer's protected health information (PHI) and the confidentiality of business data. You must know and understand the "IT – Computer, Network and Internet Usage Policy." This policy is available in Policy Tech.

lock to learn each role.

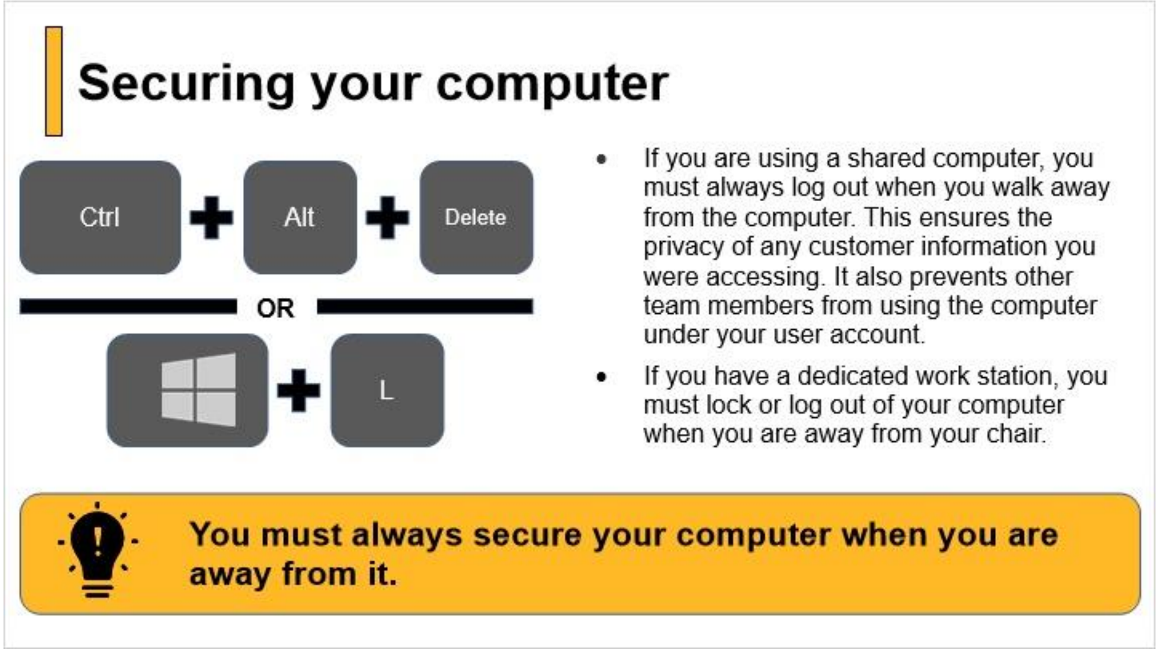
Created by Vishal patel from Noun Project



Access to NMH Computer Systems

Your job role will determine the type of access you have to the NMH computer systems.

- All team members need a password to log into the IT systems.
- You must always keep your password private. Do not post or share your password. If you suspect that your password has been used by someone else, change it immediately and contact IT Support Desk at 763-581-2580.



Securing your computer

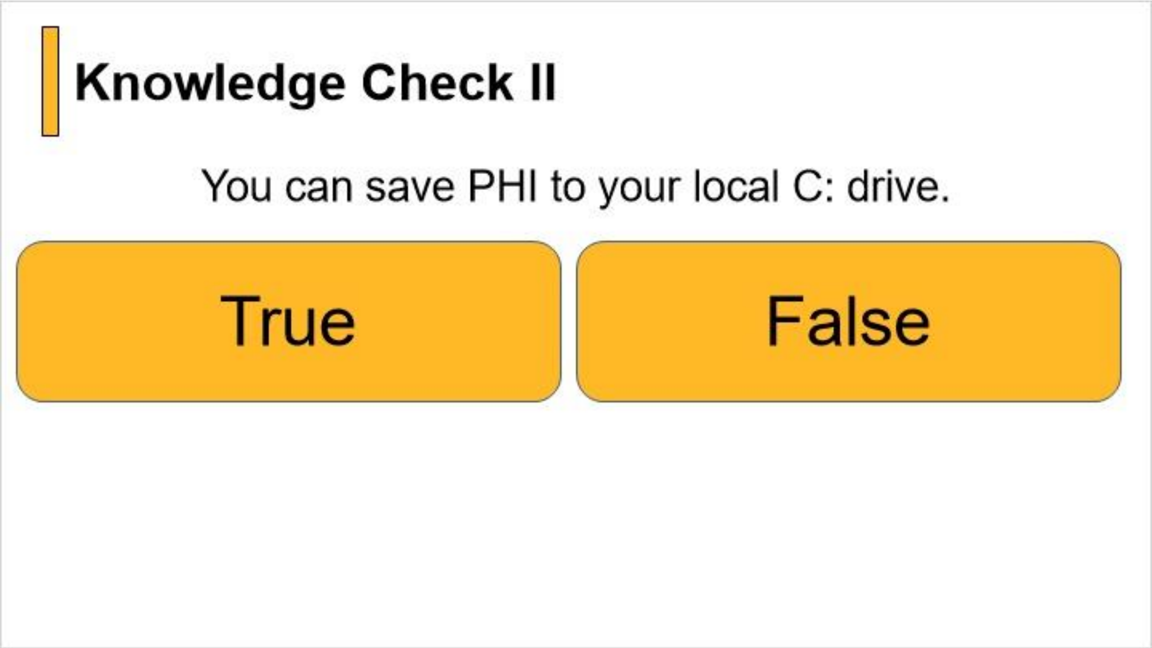
Ctrl + Alt + Delete

OR

+ L

- If you are using a shared computer, you must always log out when you walk away from the computer. This ensures the privacy of any customer information you were accessing. It also prevents other team members from using the computer under your user account.
- If you have a dedicated work station, you must lock or log out of your computer when you are away from your chair.

You must always secure your computer when you are away from it.

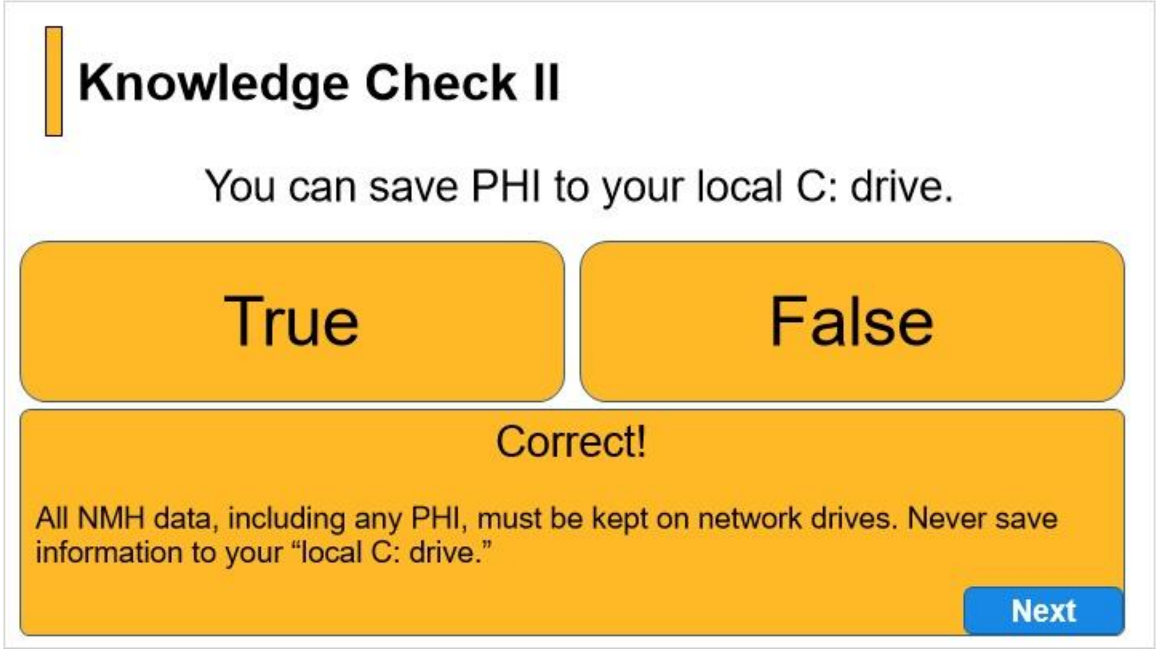


Knowledge Check II

You can save PHI to your local C: drive.

True

False

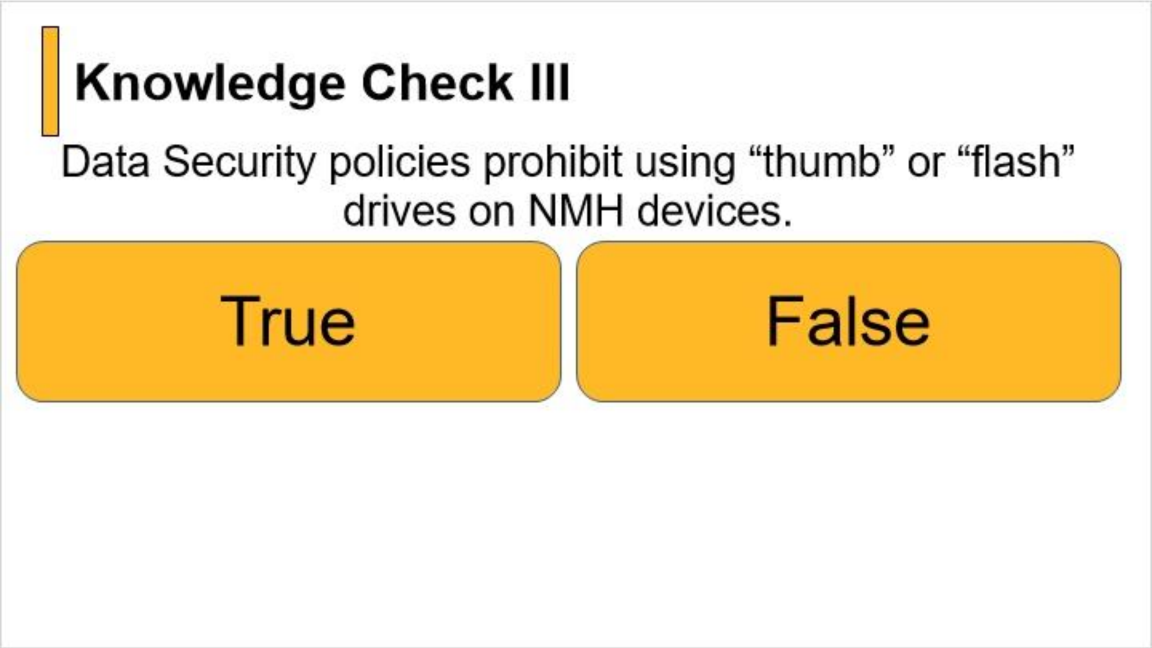


Knowledge Check II

You can save PHI to your local C: drive.

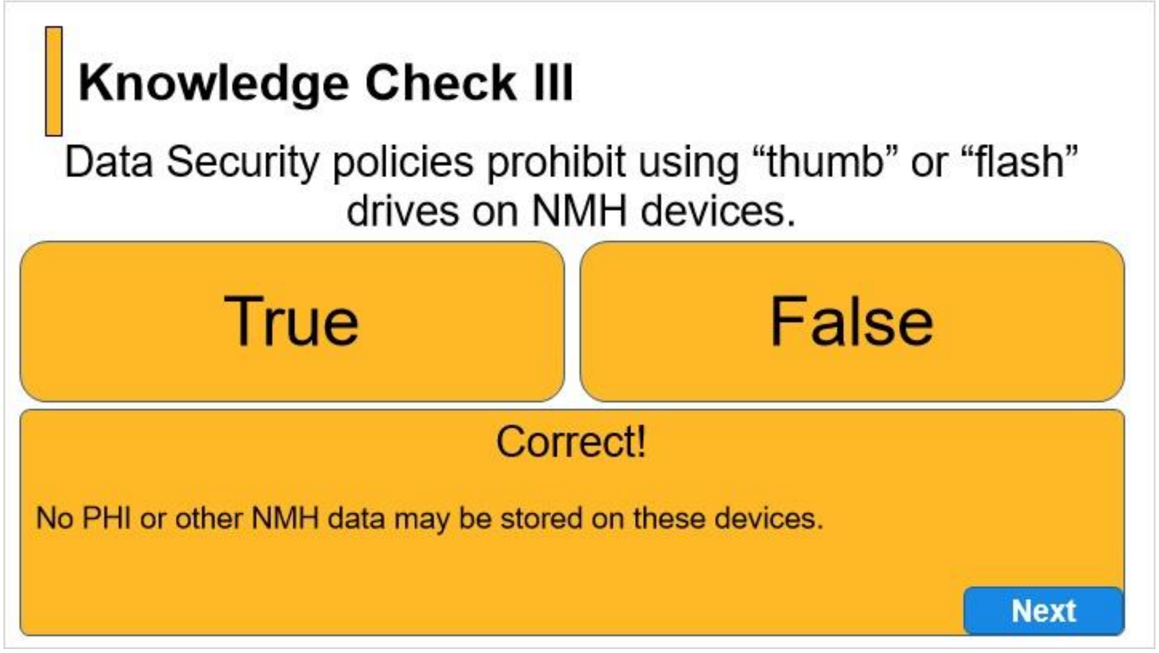
Correct!

All NMH data, including any PHI, must be kept on network drives. Never save information to your “local C: drive.”



Knowledge Check III

Data Security policies prohibit using “thumb” or “flash” drives on NMH devices.

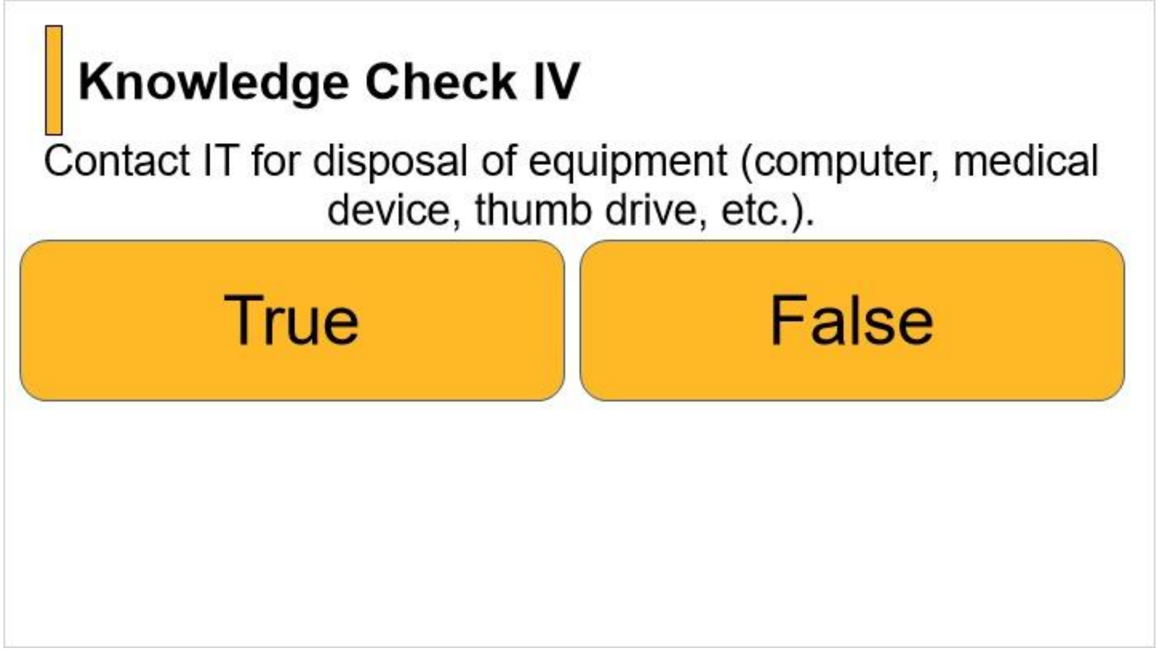


Knowledge Check III

Data Security policies prohibit using “thumb” or “flash” drives on NMH devices.

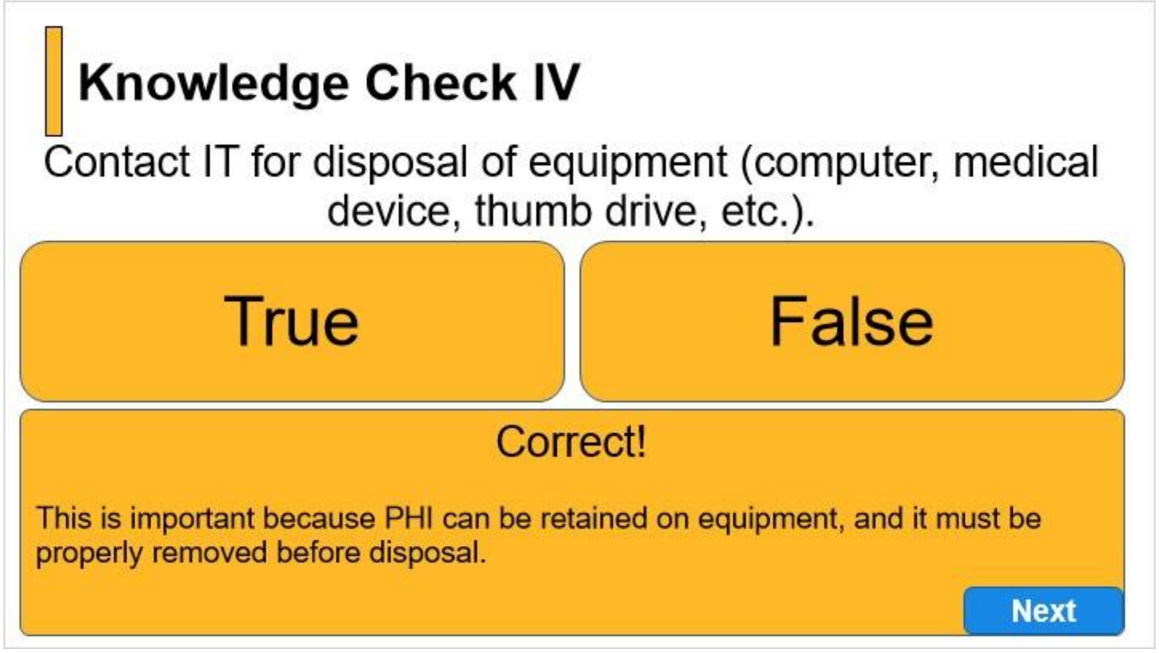
Correct!

No PHI or other NMH data may be stored on these devices.



Knowledge Check IV

Contact IT for disposal of equipment (computer, medical device, thumb drive, etc.).



Knowledge Check IV

Contact IT for disposal of equipment (computer, medical device, thumb drive, etc.).

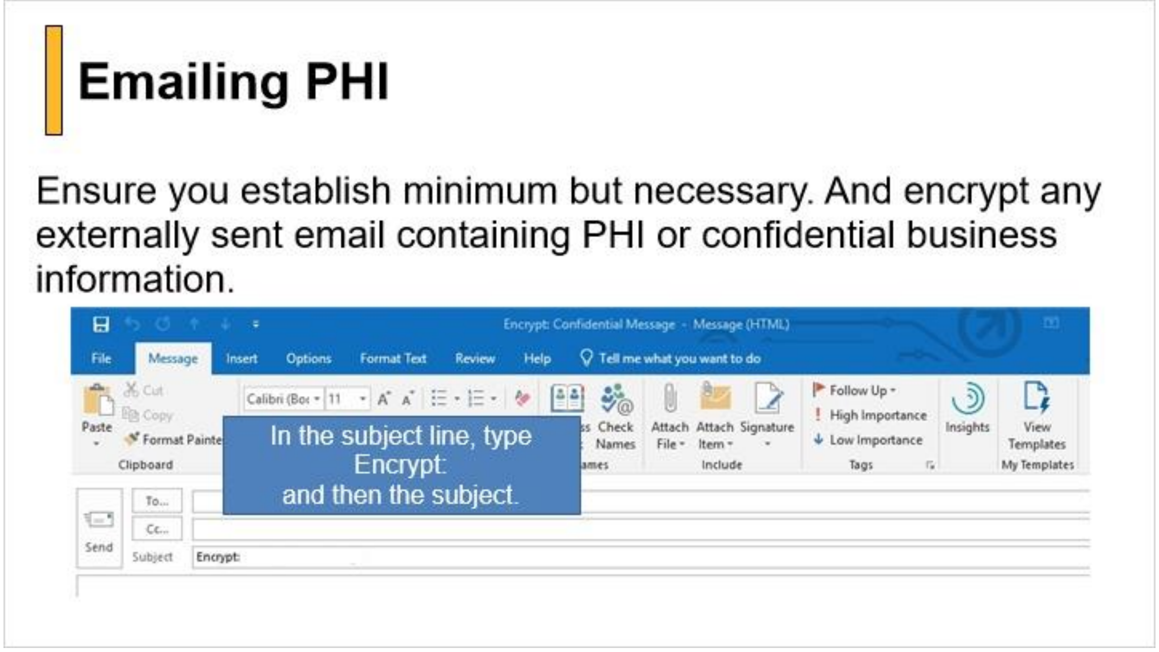
True

False

Correct!

This is important because PHI can be retained on equipment, and it must be properly removed before disposal.

Next



Emailing PHI

Ensure you establish minimum but necessary. And encrypt any externally sent email containing PHI or confidential business information.

In the subject line, type Encrypt: and then the subject.

Subject: Encrypt:

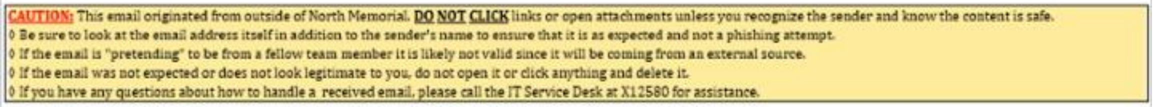
Phishing Awareness

The scenario at the very beginning of this module is an example of phishing. Data phishing is an attempt to gather sensitive information, such as usernames and passwords, often for malicious reasons, by pretending to be a trustworthy entity.

The most common phishing attempts are email and text message.

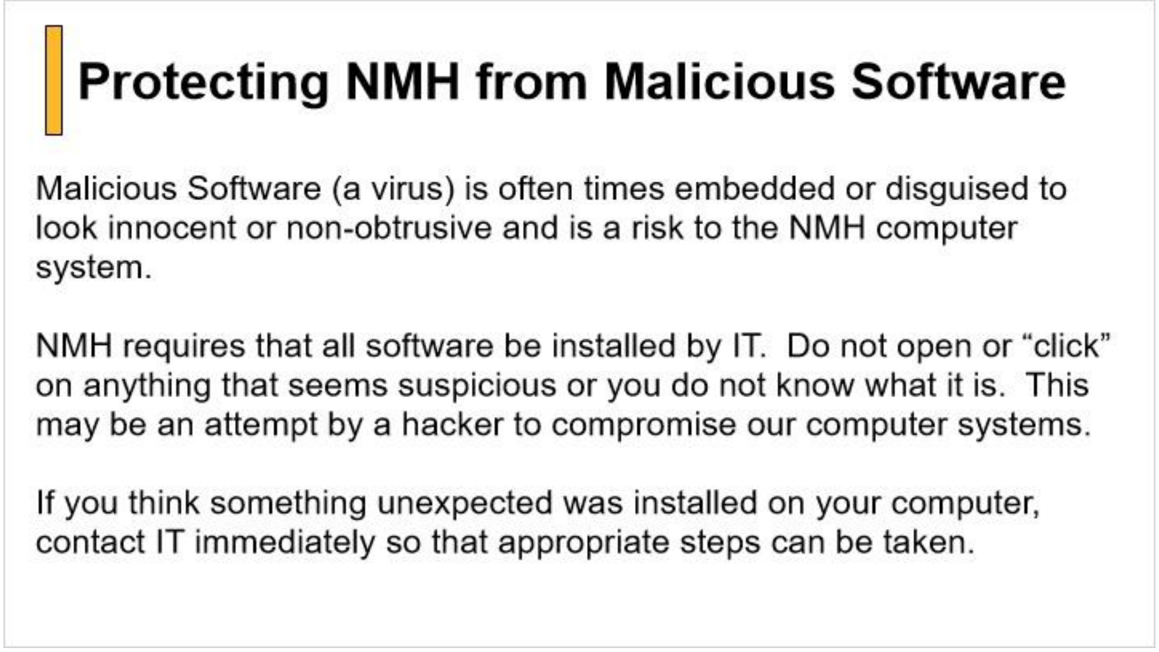
Never open emails or attachments if you do not recognize the sender.

NMH Mail from External Sources



CAUTION: This email originated from outside of North Memorial. **DO NOT CLICK** links or open attachments unless you recognize the sender and know the content is safe.
◊ Be sure to look at the email address itself in addition to the sender's name to ensure that it is as expected and not a phishing attempt.
◊ If the email is "pretending" to be from a fellow team member it is likely not valid since it will be coming from an external source.
◊ If the email was not expected or does not look legitimate to you, do not open it or click anything and delete it.
◊ If you have any questions about how to handle a received email, please call the IT Service Desk at X12580 for assistance.

The above banner appears on ANY email originated outside of NMH. When this banner appears, you know it is from outside of NMH and to only open if you know it's from a safe source and that it is not a spoofed email.

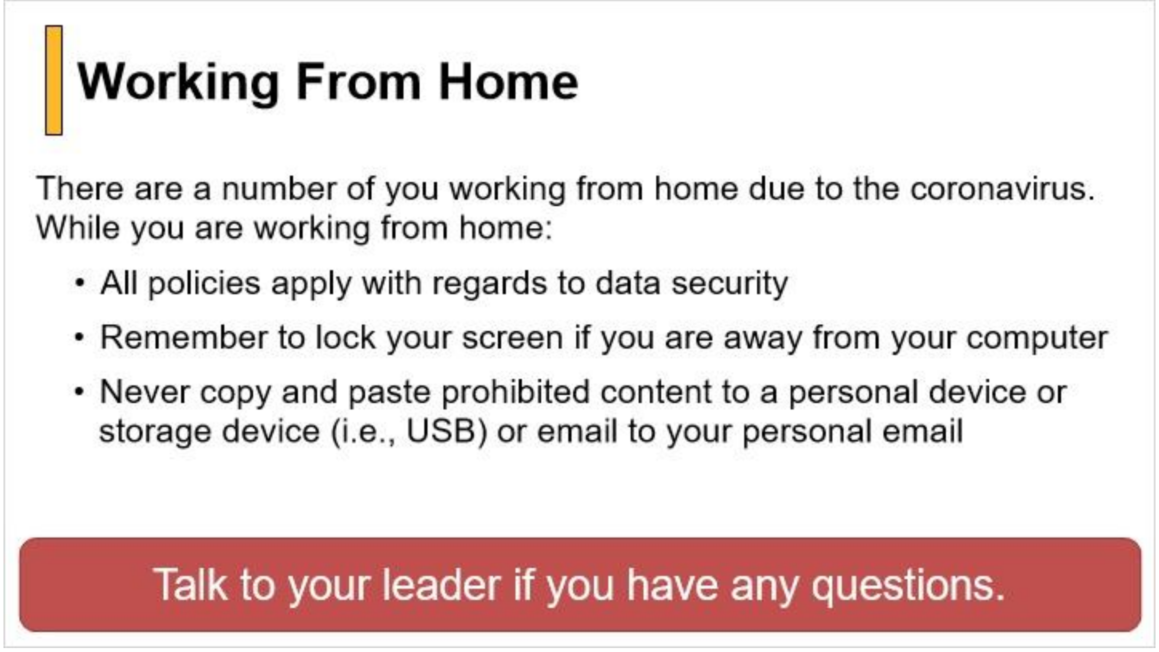


Protecting NMH from Malicious Software

Malicious Software (a virus) is often times embedded or disguised to look innocent or non-obtrusive and is a risk to the NMH computer system.

NMH requires that all software be installed by IT. Do not open or “click” on anything that seems suspicious or you do not know what it is. This may be an attempt by a hacker to compromise our computer systems.

If you think something unexpected was installed on your computer, contact IT immediately so that appropriate steps can be taken.

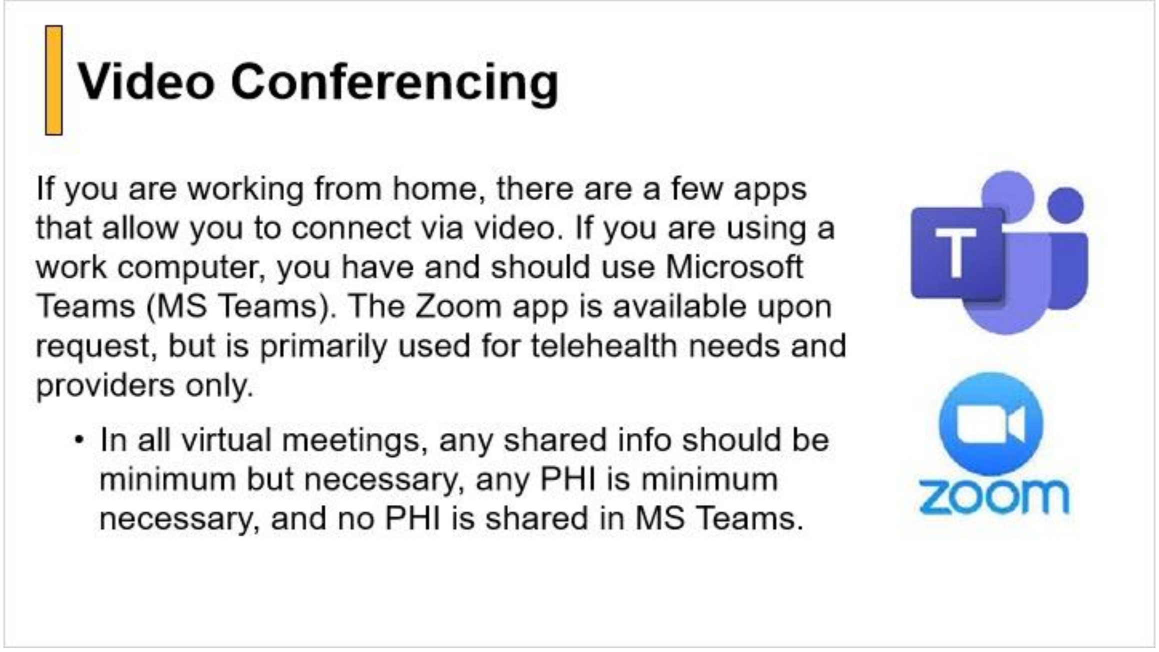


Working From Home

There are a number of you working from home due to the coronavirus. While you are working from home:

- All policies apply with regards to data security
- Remember to lock your screen if you are away from your computer
- Never copy and paste prohibited content to a personal device or storage device (i.e., USB) or email to your personal email

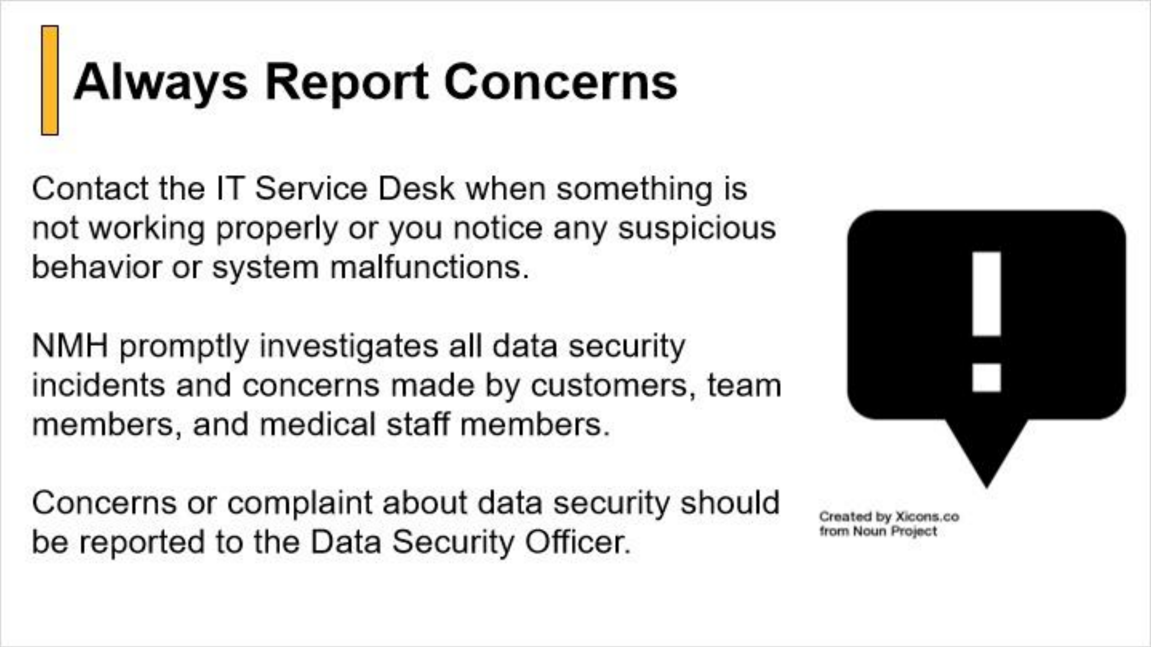
Talk to your leader if you have any questions.



Video Conferencing

If you are working from home, there are a few apps that allow you to connect via video. If you are using a work computer, you have and should use Microsoft Teams (MS Teams). The Zoom app is available upon request, but is primarily used for telehealth needs and providers only.

- In all virtual meetings, any shared info should be minimum but necessary, any PHI is minimum necessary, and no PHI is shared in MS Teams.



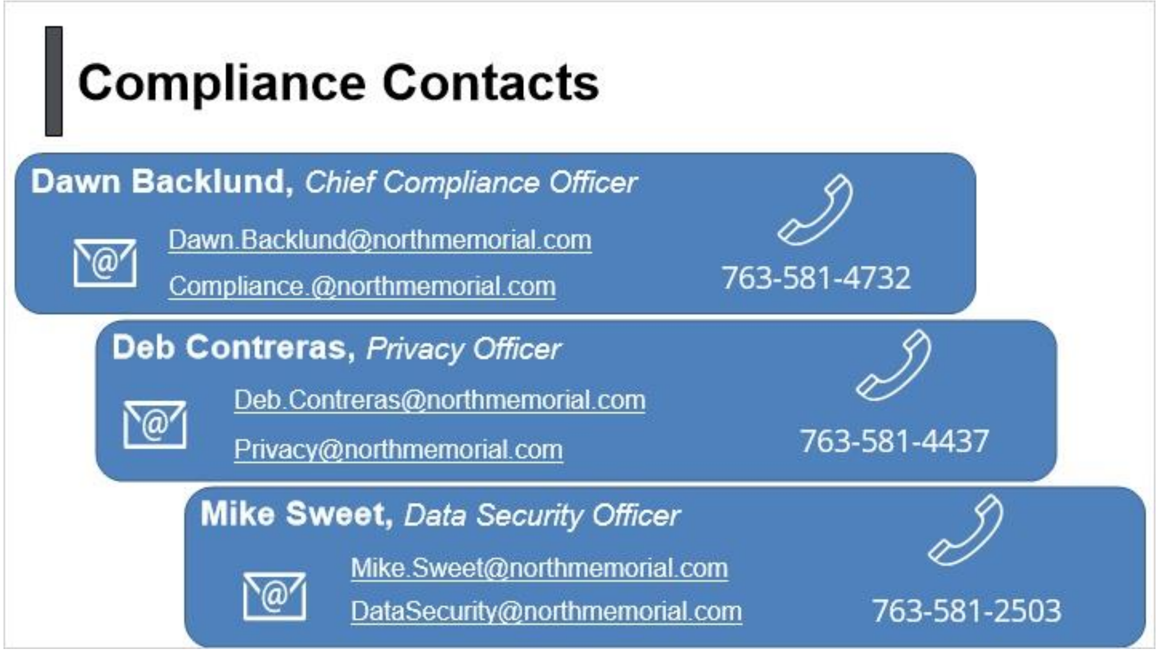
Always Report Concerns

Contact the IT Service Desk when something is not working properly or you notice any suspicious behavior or system malfunctions.

NMH promptly investigates all data security incidents and concerns made by customers, team members, and medical staff members.

Concerns or complaint about data security should be reported to the Data Security Officer.

Created by Xicons.co
from Noun Project



Compliance Contacts

Dawn Backlund, *Chief Compliance Officer*

✉ Dawn.Backlund@northmemorial.com
Compliance.@northmemorial.com

☎ 763-581-4732

Deb Contreras, *Privacy Officer*

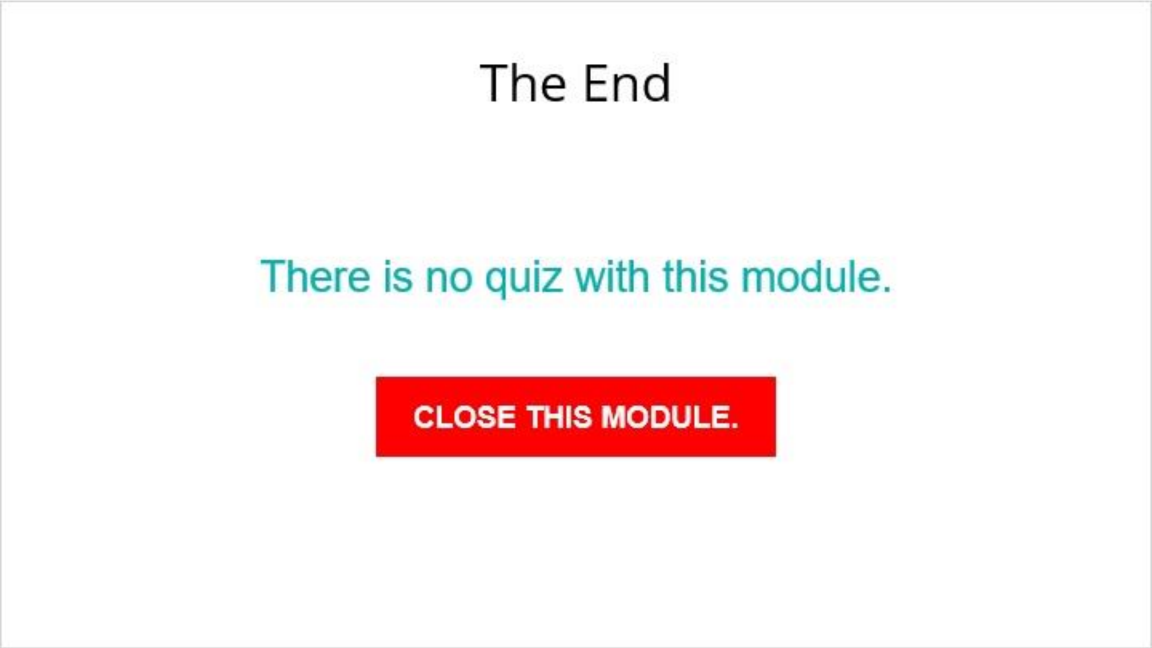
✉ Deb.Contreras@northmemorial.com
Privacy@northmemorial.com

☎ 763-581-4437

Mike Sweet, *Data Security Officer*

✉ Mike.Sweet@northmemorial.com
DataSecurity@northmemorial.com

☎ 763-581-2503



The End

There is no quiz with this module.