NORTH MEMORIAL HEALTH

2018 Data Security Training

As a NMH team member, you are responsible for protecting the security of customer information and business data.

You must also protect the security of NMH information systems.

This this module helps you understand your responsibilities related to data security.

NORTH
MEMORIAL HEALTH

Data Security

The NMH Data Security Program provides controls to ensure that that customer health records and business data is kept secure.

Our Information Technology (IT) team members play a critical role in data security. You also play a critical role.

The next slides explain IT’s role and your role in data security.

NORTH
MEMORIAL HEALTH

IT’s Role in Data Security

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.
- Monitors access and abnormal activity on IT systems (internet browsing, network storage, application clicks, email, etc.).

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

NORTH
MEMORIAL HEALTH

Your Role in Data Security

Every NMH Team Members must follow 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.

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.

NORTH MEMORIAL HEALTH

Your Role in Data Security

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

- 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 may lock your computer quickly by pressing Control/Alt/Delete or the “Windows” and “L” keys at the same time.

NORTH MEMORIAL HEALTH

Your Role in Data Security

All NMH data, including any PHI, must be kept on network drives.

- Never save information to your “local C: drive.”
- Data Security policies prohibit using “thumb” or “flash” drives on NMH devices. No PHI or other NMH data may be stored on these devices.
- Never email NMH data to a personal email address or store it on a personal device.
- Contact IT for disposal of equipment (computer, medical device, thumb drive, etc.). This is important because PHI can be retained on equipment, and it must be properly removed before disposal.

NORTH MEMORIAL HEALTH

PHI and Email

You must never email PHI outside of the North Memorial Outlook email system.

If your job requires you to email PHI to recipients outside of NMH/MGH, you must obtain access to the secure (encrypted) email system.

- PHI must only sent via the secure email system to external recipients.
- Contact your supervisor and IT for access.
- Team members who have access to this system can find locate it within the NMH Portal.

NORTH
MEMORIAL HEALTH

Protecting NMH from Malicious Software

Malicious Software (a virus) is a risk because if it is installed it creates vulnerabilities to the NMH computer system.

NMH requires that all software be installed by IT. You cannot install software on any NMH device. You must contact IT if you have a software installation need.

NORTH
MEMORIAL HEALTH

Protecting NMH from Malicious Software

Only browse work related websites at work.

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.

NORTH
MEMORIAL HEALTH

Phishing Awareness

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 messages.

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

NORTH
MEMORIAL HEALTH

Downtime Procedures

All clinical areas have downtime procedures to ensure that if there is a computer outage, team members can continue to provide and document clinical care.

You must learn your area's Downtime Procedures.

- Downtime Read Only access applies if the Epic system is down.
- Downtime workstation and "black box" procedures apply if the IT/computer systems are down.

NORTH MEMORIAL HEALTH

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.

NORTH
MEMORIAL HEALTH

Compliance Contacts

Kelsey Brodsho, *Chief Compliance Officer*
Kelsey.Brodsho@northmemorial.com
compliance@northmemorial.com
763.581.0976

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

NORTH
MEMORIAL HEALTH