# NMHC HIPAA Security Training

*2017 Version*

NORTH
MEMORIAL HEALTH

# HIPAA Data Security

HIPAA Data Security is intended to provide the technical controls to ensure electronic Protected Health Information (PHI) is kept secure and private. There are three primary sections to HIPAA Data Security:

- **Administrative Safeguards**
  - Assign security responsibility to a Data Security Officer – Mike Sweet
  - Regularly identify, define and prioritize risks to maintaining the confidentiality, integrity and availability of our information systems containing PHI. IT performs risk assessments annually to identify risks.
  - Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures.
- **Technical Safeguards**
  - Technical controls in place to protect ePHI.
- **Physical Safeguards**
  - Controls in place to protect the IT systems that house PHI and the transition of PHI to ensure the PHI is protected both at rest and in motion.

# Access Authorization

- Access to IT resources require a request from management of the team member's area and approved by IT.
- IT will then create a Login for the requested individual with restricted access and rights associated to their role.
- Exceptions to the standard role based access must be requested by management and approved by IT.
- Parameters for how access is given and managed are dictated by IT policies.
  - IT-Computer, Network and internet Usage Policy
  - IT-Computer System Access & Password Controls Policy

# Modifying or Termination of Access

- Modification to the standard role based access must be requested by management and approved by IT.
- IT terminates access based on specific requests submitted by management, the Human Resources termination report sent over weekly, or in specific coordination with Human Resources.
- Parameters for how access is modified and terminated are dictated by IT policies.
  - IT-Computer, Network and internet Usage Policy
  - IT-Computer System Access & Password Controls Policy

# Remote Access

Remote Access is the ability to connect to North Memorial IT resources while not on the North Memorial network. Since Remote Access by it's nature inherently creates risk due to the exposure created by anyone being able to attempt access, different technology is used to provide this access and tighter controls are implemented to manage it.

- North Memorial allows end users and business associates Remote Access as needed through a specialized secure portal by request only.
- Printing and local computer access are not allowed via Remote Access. If there is a need for either it requires an exception approved by IT.
- Direct Remote Access to systems is only granted to specific support resources as determined by IT and approved by the Data Security Officer.
- If Remote Access is a required business need contact IT to request it.

# Unique User Identification & Password Expectations

- Logins and Passwords are a key defense against unauthorized access of PHI. North Memorial requires every individual accessing computing resources to have a unique login and password. See policies:
  - IT-Computer, Network and internet Usage Policy
  - IT-Computer System Access & Password Controls Policy
- General Login-Password rules:
  - Login is set by IT and is a standard format issued to the end user
  - Passwords are created by end user, must follow IT standards for complexity and format
  - Passwords will expire and can't be reused
  - Passwords must not be shared or stored where they could be learned by others

# Bring Your Own Device

- In order to protect North Memorial's PHI, North Memorial provides appropriate core computing devices for customer care and business functions. However, North Memorial will allow certain users to use their own personal devices such as laptops, tablets and smartphones (referred to as BYOD) on a limited basis to access North Memorial approved applications and data.
- This is governed by the IT - Mobile Device Management - Bring Your Own Device (BYOD) Policy.
- Contact IT to request this access if there is a business reason for it.

# Workstation & Internet Use

- North Memorial IT provides workstations, Internet, applications, and network access to workers to perform their jobs.
- These resources are the property of North Memorial and users are required to follow the IT Computer Network and Internet Usage Policy.
- Users need to follow all aspects of the policy, related specifically to protecting PHI:
  - Do not store any PHI on workstations, thumb drives, or anywhere other than the North Memorial network or applications.
  - Log out of your workstation when not in use.
  - Shut down your workstation at the end of each day.
  - Do not engage in any non-work related Internet use.
  - Report any suspicious behavior or issues to IT.

# Email Use Expectations

Team members with a business need will be granted an e-mail account. The granting of an e-mail account requires that the user assigned the account be subject to certain standards regarding its appropriate use. This includes, but is not limited to, the following:

- Do not send email outside of the North Memorial Outlook email system with PHI.
- Content of e-mail:
  - Confirm the content of the e-mail is business related to North Memorial.
  - Review the content for any statement that could have potential harm to North Memorial, other users, or our customers and their families.
- Appropriate audience:
  - Choose the audience and confirm e-mail is the appropriate tool for this communication.
  - Review the audience to be sure the e-mail will communicate to the complete audience required for an effective message.
- Confirming destination and responding to e-mails:
  - Before sending an e-mail, review the mailing addresses and names of individuals listed.
  - When responding to e-mails received, verify the addressees before responding “to all”.
- Do not open attachments from unknown sources. Alert North Memorial’s IT Service Desk at 763-581-2580 of any suspicious attachments or emails.

# Encryption and Decryption

North Memorial must encrypt any PHI data “while at rest or in motion”. This ensures that if it is accessed in an unauthorized manner it is unrecognizable. North Memorial IT has an Encryption Policy that establishes the parameters on how this is done. Your role in ensuring this is followed is to: Do not send email outside of the North Memorial Outlook email system with PHI.

- All PHI must be stored on a North Memorial network server that is managed by IT and all the IT policies.
- All confidential and restricted information/PHI transmitted via email to an email address outside of the North Memorial Email system must be encrypted. Contact IT if you have a need to do this.
- Any PHI data to be shared with an outside entity must go through IT or M&R so it can be encrypted.
- Do not store PHI on any desktop or laptop computer.
- Removable storage devices except those used for backup purposes must not be used for the storage of PHI. If there are exceptions approved by the Data Security Officer the removable devices must be fully encrypted.

# Social Media

- Personal use of social media (Facebook, Twitter, Snapchat, etc.) is prohibited while working.
- Team members involved with social media must use their personal email account.
- Team members **must never** represent their views and opinions as those of NMHC.
- NMHC logo, trademark or other service marks cannot be used without the consent of Business Development and Marketing.
- Respect the copyright laws and other intellectual property laws.
- Be respectful of fellow team members, business partners and competitors.
- Creating a blog group or online group related to NMHC is prohibited.
- **NEVER** disclose personally identifiable information or protected health information on social media. This includes pictures of customers, even if their face is not showing.

# Social Media

- All team members are expected to read, know and follow the Social Media policy.
- If you have any questions regarding this policy, please ask Human Resources before acting.
- Report any violation of this policy to your department manager, Human Resources, Data Security Officer, Privacy Officer, Chief Compliance Officer or Compliance Hotline. Any violations of this policy are grounds for disciplinary action, up to and including immediate termination of employment.

# Protection from Malicious Software

In an effort to obtain access to PHI or other private information, sometimes “the bad guys” distribute Malicious Software that is intended to get installed on IT systems to create vulnerabilities. North Memorial requires that all software be installed by IT as per the IT Computer Network and Internet Access Policy.

- Do not install software on any North Memorial computing device.
- If you need software installed contact IT.
- Do not open or “click” on anything that seems suspicious or you do not know what it is.
- If you do incur an instance that something unexpected appears to be installing on your North Memorial computing devices contact IT immediately.

# Phishing Awareness

- Data Phishing is the attempt to gather/acquire sensitive information such as usernames, passwords, financial information, often for malicious reasons, by masquerading as a trustworthy entity.
- There are many forms and types of phishing, but the most common forms of phishing are email and text messages.
- Many “phishers” now leverage information about the people they are phishing for by using as much public information (Facebook, Twitter, websites, LinkedIn, etc.) as they can acquire about an individual to more effectively appear trustworthy and legitimate to lure someone into sharing sensitive information.
- The phisher may “time and title” the phishing scam email in a manner where it seems topically appropriate for the recipient.

# **Phishing Awareness** (continued)

Things you should do to prevent phishing.

- Verify that the sender is who they appear to be.
- Inspect the message for things that look “out of normal”.
- Search the Internet for some key words to see if this is a known scam.
- When in doubt contact IT and report the issue so IT can investigate.

# Media Disposal and Re-Use

- Computing media that may contain PHI must be adequately obscured, erased, destroyed, or otherwise rendered unusable prior to disposal or reuse.
- Contact IT for disposal of any North Memorial IT equipment at 763-581-2580.
  - All decommissioned media must be stored in a secure area prior to destruction.
  - Media reuse and destruction practices must be tracked and documented.
  - Encrypted media is not exempt from this policy.
  - All information must be destroyed when no longer needed.

# Facility Access Control

North Memorial must protect the IT computing environment from unauthorized physical access . North Memorial IT has a Physical Security Policy to establish the rules for the granting, control, monitoring, and removal of physical access to IT facilities.

- Access to IT facilities must be granted only to North Memorial support personnel and contractors whose job responsibilities require access to that facility.
- All facility entrances, where unauthorized persons could enter the premises, must be controlled.
- Equipment must be protected from power failures and other disruptions caused by failures in utilities.
- Signage for restricted access rooms and locations must be practical, yet minimally discernible evidence of the importance of the location.
- All IT facilities that allow access to visitors will track visitor access with a sign in/out log.
- Card access records and visitor logs for IT facilities must be kept for routine review based upon the criticality of the IT being protected.
- Visitors in card access controlled areas of IT facilities must be accompanied by authorized personnel at all times.
- The person responsible for IT physical facility management must review access records and visitor logs for the facility on a periodic basis and investigate any unusual access.

# Data Back Up Plan

- North Memorial must protect PHI/data from being either intentionally or unintentionally destroyed. While there are many steps being taken to prevent this from occurring, should it happen we need a functional and current Back Up of the data.
- North Memorial IT performs backups of all data on the network on a daily, weekly, and monthly basis as appropriate to provide the ability to restore data if needed. Copies of the data are stored at an undisclosed offsite location and are securely transported daily.

# Emergency Access Procedure

IT systems may become unavailable for many reasons. Should this occur it is important that end users dependent on those systems to perform their job in real time are able to continue working without those systems/data available. Users should know, practice, and follow the Epic System Downtime Procedures Policy.

- Site leadership and IT will collaborate to determine to call a “Downtime”.
- Customer Care areas should find the required forms in the department Downtime box.
- If Epic is down, but the computer is still functioning users should access Epic Downtime Read Only to see pertinent customer information and use their Downtime Box for all paper processes needing to be followed.
- If all computer access is down, users should go to their Downtime Computer and print current reports for their area.
- Once systems are restored data will need to be loaded and then an “All Clear” will be called and users may access Epic again.

# Disaster Recovery Plan

- North Memorial has many system redundancies as appropriate, dual data centers, and IT formally manages all applications and IT services relative to their impact to customer care and operations.
- When an interruption to those services does occur, the IT Major Incident Policy is followed.
  - An event is classified as a Major Incident when systems critical to customer care experience an interruption exceeding thirty (30) minutes.
  - A Major Incident may be declared immediately if IT or Business Leadership determines the incident is unlikely to be resolved within thirty (30) minutes.
  - Impacted areas should immediately refer to and follow their department downtime/backup procedures. If Epic is impacted, follow the *Epic System Downtime Procedures.*

# Access Monitoring and Audit Controls

- North Memorial needs to monitor access and any abnormal activity on systems that contain PHI. IT has a Logging, Monitoring, and Alerting Policy that is followed to ensure that appropriate systems have the capabilities to do this.
- This includes but is not limited to:
  - Systems that contain PHI,
  - Internet browsing,
  - Systems that are critical to IT services,
  - email, and network storage.
- IT may access and use this information at any time and does so on a regular basis when investigating data security incidents or other IT systems related issues.

# Reporting a Security Incident

- NMH has the responsibility for investigating all data security incidents/ complaints/concerns made by customers, team members, members of the medical staff, etc.
- Investigations are performed internally by the Data Security Officer.
- Concerns/complaints should be reported to the Security Officer at DataSecurity@northmemorial.com or 763.581.2580.

# Breach Notification Process

- A Breach is the acquisition, access, use or disclosure of unsecured protected health information (PHI) in a manner that compromises the security or privacy of the PHI.
- All Team Members must be mindful of potential privacy incidents and report any suspicious or questionable activity regarding inappropriate use or disclosure of customer information.
- The Privacy Officer assures that North Memorial identifies breaches of PHI, notifies the appropriate parties, and takes other necessary steps regarding mitigation and compliance.

# Breach Notification Process

Report Breaches to the Privacy Officer directly, or by contacting your manager, Human Resources, Chief Compliance Officer, Data Security Officer, or the Compliance helplines:

- North Memorial: 763-581-4670 or compliance@northmemorial.com
- Maple Grove Hospital: 763-581-1575 or mghcompliance@maplegovehospital.com
- E-mail to HIPAA.Inquiries@northmemorial.com or datasecurity@northmemorial.com

# Your role in ensuring HIPAA Data Security…

Know and understand the
**IT - Computer, Network and Internet Usage Policy**

- Keep your password private, never post or share.
- **Never** email PHI outside of the North Memorial Outlook email system.
- Only browse work related websites while at work.
- Never open emails or attachments that you do not recognize the sender.
- Log out of your computer when you are done or will be away for more than a couple minutes.
- Lock your computer if you need to step away for more than a couple of minutes using Control/Alt/Delete or the “windows” and “L” keys.

# Your role in ensuring HIPAA Data Security…

- Keep any data on the network drives.
- **Never** try and save information to your local C: drive.
- **Never** save any data to a “thumb drive” or burn to a disk.
- In public areas make sure computer monitors are turned away from view and have privacy screens as needed.
- Know and practice your Downtime Procedures.
- Contact the Service Desk when something isn’t working properly or you notice any suspicious behavior so IT can look into it.