Document Owner:	**Reviewed By:**	**Approved By:**
Director, IT Infra Data Security Officer	VP, Information Sys & CIO, Chief Compliance Officer, IT Governance Board	NMH System Leadership Team (SLT)

SCOPE

This Policy and Procedure applies to:
Ambulance Services
Clinic Services
Home and Community Services
Maple Grove Hospital
North Memorial Medical Center

POLICY

North Memorial Health Care considers access to its computer network, whether through equipment provided by North Memorial directly in the workplace or by the granting of access by other means, to be a critically important resource. As such, it is required that individuals (users) granted access to North Memorial's computer network will follow North Memorial's policy and procedures and conduct themselves in a manner that is consistent with established legal and ethical guidelines.

"Access" includes both those systems, applications, tools, or other means made available directly within the North Memorial computing network and those additional resources indirectly made available as a result providing a connection to the public Internet. In order to effectively and efficiently manage North Memorial resources (human, financial, computing assets, and data) and comply with mandated Health Information data management standards, network access must necessarily be subject to certain restrictions.

Therefore, in order to protect North Memorial, its resources, team members, medical staff, customers and business associates, all users granted access to the network must comply with all of the following "Procedures & Guidelines":

PROCEDURE

A. Permitted Use of Internet and North Memorial Computer Network

- The computer network including, but not limited to the information, files and data transmitted by or stored on the computer network is the sole property of North Memorial and is to be used for business purposes. Users are provided access to the computer network to assist them in the performance of their jobs. Additionally, users may also be provided with access to the Internet through the computer network. All users are required to use North Memorial's computer resources and the Internet in a professional, lawful and ethical manner. Abuse and any personal or other use of the computer network or the Internet North

Memorial deems inappropriate or excessive, may result in North Memorial Performance Improvement Process action, up to and including possible termination, and/or criminal liability. Inappropriate use includes, but is not limited to, insensitive jokes, offensive pictures or messages, defamatory comments, virus propagation, or other abuse or misuse of North Memorial's computer network.

All North Memorial data is to be stored on the network to protect it. No personal or company data should reside on a workstation or laptop hard drive (C:), CDs, DVDs or memory sticks.

- Social Media usage: Please see the Social Media policy.

B. **Computer Network Use Limitations**

- Prohibited Activities:

Without prior written permission from North Memorial, the computer network may not be used to disseminate, view or store commercial or personal advertisements, solicitations, promotions, destructive code (e.g., viruses, trojan horse programs, etc.) or any other unauthorized materials. Workers must not under any circumstance use North Memorial's computer network to engage in any conduct that violates the law, any policy of North Memorial, or is inconsistent with North Memorial's interest.

- Personal Use:

Occasional limited appropriate personal use of the computer must not a) interfere with the user's or any other worker's job performance; b) have an undue effect on the computer or the network's performance; c) or violate any provisions, guidelines or standards of this agreement policy or any other of North Memorial.

- Illegal Copying:

Workers may not illegally copy material protected under copyright law or make that material available to others for copying. Workers are responsible for complying with copyright law and applicable licenses that may apply to software, files, graphics, documents, messages, and other material you wish to download or copy. Workers may not agree to a license or download any material for which a registration fee is charged without first obtaining the express written permission of North Memorial.

- Communication of Trade Secrets:

Unless expressly authorized to do so, user is prohibited from sending, transmitting, or otherwise distributing proprietary information, data, trade secrets or other confidential information (this would

include, but not be limited to, establishing a personal web page with North Memorial logos and name) belonging to North Memorial.

C. **Software Support**

- Software support will be provided for all standard software products utilized within North Memorial. Any request for "non-standard" software products must be requested by using the IS Request Process and approved for a valid business need by IT.

- If unsupported or unauthorized software is found or suspected of contributing to operational problems of a computer, the software may be disabled and uninstalled at the need and discretion of Information Technology, in order to resolve problems.

D. **Duty Not to Waste or Damage Computer Resources**

- Accessing the Internet:

The Internet is a worldwide network of computers that contains millions of pages of information. Users are cautioned that many of these pages include offensive and inappropriate material. Even innocuous search requests may lead to sites with highly offensive content. Additionally, having an e-mail address on the Internet may lead to receipt of unsolicited e-mail containing offensive content. Users accessing the Internet do so at their own risk and North Memorial is not responsible for material viewed or downloaded by users from the Internet.

- Frivolous Use:

Computer resources are not unlimited. Network bandwidth and storage capacity have finite limits, and users connected to the network have a responsibility to conserve these resources. As such, the user must not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but are not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet (i.e., Facebook, Craigslist, Twitter, etc.), playing games, engaging in online chat groups, uploading or downloading large files, accessing streaming audio and/or video files unnecessarily, or otherwise creating unnecessary loads on network traffic associated with non-business-related uses.

- Virus Detection:

Files obtained from sources outside North Memorial, including disks brought from home, files downloaded from the Internet, newsgroups, bulletin boards, other online services, files attached to personal e-mail (ie: Hotmail, Yahoo, etc), and files provided by customers or vendors, may all contain dangerous computer viruses that may damage North Memorial's computer

network. Users should never download these files to the North Memorial network without contacting IT to ensure the material can be evaluated or approved by virus checking software. Users who suspect that a virus has been introduced into North Memorial's network, must notify North Memorial's IT Service Desk at 763-581-2580 immediately.

E. **Electronic Mail (e-mail)**

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:

- 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.

F. **No Expectation of Privacy**

- Users are given computer and Internet access to assist them in the performance of their jobs. The computer network and equipment, including but not limited to the information, files and data transmitted by or stored on them are the sole property of North Memorial. Users have no expectation of privacy in anything they create, store, send or receive using North Memorial's computer equipment or network.

- Users expressly waive any right of privacy in anything they create, store, send or receive using North Memorial's computer equipment, network or Internet access.

- North Memorial has the right to, and in fact does, monitor and log any and all

aspects of its computer system including, but not limited to, monitoring Internet sites visited by users, monitoring chat and newsgroups, monitoring file downloads, and all communications sent and received by users. North Memorial may inspect, review, retain, disclose and/or use any and all materials (including, but not limited to both incoming and outgoing e-mail messages) created, stored, sent or received by users through any company network or Internet connection.

- North Memorial has the right to utilize software that makes it possible to identify and block access to Internet sites containing material deemed inappropriate in the workplace.

G. **Access Codes and Passwords**

- The confidentiality and integrity of data stored on North Memorial computer systems must be protected by access controls to ensure that only authorized users have access. This access shall be restricted to only those capabilities that are appropriate to each user's job duties.

- Details regarding computer access and passwords may be obtained by requesting a copy of the Information Technology department policy, Computer System Access & Password Controls.

H. **IT Responsibilities**

- IT management shall be responsible for the administration of access controls to all North Memorial computer systems. Access to North Memorial computer systems will not be granted unless the user signs an IT Network Acknowledgment & Consent Form.

Worker/User Responsibilities

Each worker/user:

- Is encouraged to attend classes to learn basic skills and knowledge about North Memorial applications.

- Shall not add/modify hardware (i.e. speakers, sound cards, printers, etc.) or add any software without IT approval.

- Shall not store personal or company data on a workstation/laptop hard Drive (C:), CD or DVD, memory stick, or any other portable media.

- Upon learning of any violation of this policy, users should notify IT.

- Shall be responsible for all computer transactions that are made with his/her User ID and password. Shall not disclose passwords to others.
- Passwords must be changed immediately if it is suspected that they may have become known to others.
- Passwords should not be recorded where they might be easily obtained.
- Shall be subject to any established procedures regarding periodic changing of password(s).
- Shall use passwords that will not be easily guessed by others.
- Shall log out when leaving a workstation for an extended period.
- Computer/Work Stations. Computer monitors must be positioned away from common areas or a privacy screen must be installed to prevent unauthorized access or observation. The screens on unattended computers must be returned to the main menu or to a password protected screen saver.

I. Human Resources Responsibility

Human Resources will notify IS management promptly whenever an team member leaves North Memorial or transfers to another department so that his/her access can be changed or revoked as appropriate. Involuntary terminations must be reported concurrent with the termination.

J. Consent

By using North Memorial's computer network, worker/users consent to the terms of this policy. If workers/users receive information, files or data from outside sources of North Memorial on North Memorial's equipment or using North Memorial's resources, such information, files and/or data are subject to the terms of this policy.

K. Not a Contract

North Memorial reserves the right to change or depart from this policy at any time, with or without notice. This policy does not constitute, and shall not be construed as, a contract of employment.

L. Violation

As stated elsewhere in this policy, any violation of this policy may result in disciplinary action, up to and including discharge, and other legal action.

M. **Exceptions**

Exceptions to this policy require a formal documented request sent to the IT Chief Data Security Officer for authorization and it must be documented with the Data Security Analyst. Contact your IT Business Analyst for detailed information and forms.

Cross Reference:
Computer System Access & Password Controls Policy
NMHC Code of Conduct

TABLE OF REVISIONS

Date	Description of Change
10/20/16	Removed reference to policy # in section G, 2nd bullet point. Added approval date in footer.
Dec 2016	Changed "staff" to "team member" and "Patient" to "Customer" & reformatted for ease of reading.
08/2018	No Changes- Periodic Review