NEWTON MEDICAL CENTER NEWTON, KANSAS 67114 **INFORMATION TECHNOLOGY** POLICY/PROCEDURE	DOCUMENT ID: 16108 RESPONSIBLE PARTY: **INFORMATION TECHNOLOGY DIRECTOR** PUBLISHED DATE: 6/17/2019 9:36:53 AM PAGE 1 of 10
TITLE: **NMC HIPAA Workstation Use and Security Policy**	

1.0. PURPOSE:

1.1. Newton Medical Center (NMC) is committed and required to provide security to protect its computerized clinical and business information systems. Its computer system hardware and software as well as the information and data carried by the system are the sole property of NMC. Any misuse of NMC workstations may result in withdrawal of access to the system or NMC information or data.

1.2. To document requirements for acceptable Workstation use.

2.0. SCOPE:

2.1. This policy applies to all members of the NMC community. Members of the NMC community include but are not limited to:

Workforce Member: an individual performing work on behalf of NMC and under the direct control of NMC, whether or not the member is employed by NMC. Examples include staff; temporary agency workers; students; contractors; clergy; volunteers; and Board members.

Extended Community Member: an individual who is present on NMC premises or accessing information resources at NMC for a specific treatment, payment, or health care operation business purpose allowed under the Health Insurance Portability and Accountability Act (HIPAA) such as a third party payer representative, a visitor for a guided tour or observation experience, media or vendor representatives, or other health care providers involved in a patient's continuum of care.

Business Associate: a person or company that performs certain functions or activities on behalf of, or for, NMC that involve the creation, use, disclosure, or storage of NMC PHI.

3.0. POLICY:

3.1. Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity, and availability of sensitive information, including protected health information (PHI) and that access to sensitive information is restricted to authorized users. Workforce members using workstations shall consider the sensitivity of the information, including PHI, that may be accessed and minimize the possibility of unauthorized access.

3.2. Access Control:

3.2.1. NMC will implement Administrative, Physical, and Technical safeguards for all workstations that access electronic PHI to restrict access to authorized users.

3.2.2. Administrative

3.2.2.1. Workstation Configuration

3.2.2.1.1. NMC has established standard configurations for desktop technologies deployed throughout the organization. All computers, computer peripherals and software, as well as printers, faxes, and other miscellaneous hardware purchased with NMC funds or attached to any component of the NMC network must meet these standards.

3.2.2.1.2. The IT department shall have sole discretion in determining which hardware, operating systems, and connectivity solutions will be supported. Users may not independently install connectivity hardware or software to the computing resources of NMC.

3.2.2.1.3. All NMC Community Members must comply with NMC policies, state and federal laws and regulations regarding the proper acquisition, use and copying of copyrighted software and commercial software licenses.

3.2.2.1.4. NMC Community Members may not install unauthorized software on workstations.

3.2.2.1.5. Workstations are to be used to conduct NMC business only.

3.2.2.1.6. NMC Community Members are responsible for maintaining the integrity and privacy of the data maintained on NMC workstations by adhering to password requirements.

3.2.2.1.7. Ensure that each workstation has the necessary access controls to restrict unauthorized users and programs from accessing patient health or sensitive business information.

3.2.2.1.8. NMC reserves the right to inspect all data and to monitor the use of all its computer systems, and as such, workstation users have no right of privacy with regard to information on workstations. NMC's right of access to personally owned computing devices will be limited to NMC's patient or business information and applications important to maintaining security over that information, including, but not limited to anti-virus software, operating systems, etc. NMC reserves the right to remotely access, monitor, control, and configure workstations and any software residing on them

3.2.2.2. Asset Documentation

3.2.2.2.1. Workstations designated for transfer within or between entities will comply with accounting fixed asset procedures.

3.2.2.2.2. Workstations designated for external relocation, disposal, sale, or donation will be appropriately tracked according to NMC inventory management guidelines to ensure appropriate tracking, hardware sanitizing, and disposal.

3.2.2.3. Asset Management and Protection

3.2.2.3.1. All Workstations purchased by NMC are considered company assets throughout the life of the asset at NMC.

3.2.2.3.2. Workstations should not be relocated or changed by anyone other than authorized NMC employees or vendors.

3.2.2.3.3. Workstations will be protected on and off NMC premises.

3.2.2.3.3.1. Appropriate measures include:

- Restricting physical access to workstations to authorized personnel only
- Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access
- For all Workstations that are not located in 24/7 departments, Users should log out of all applications, and log out of the network at the end of the business day or User workday

3.2.2.3.4. Laptops and wireless device Users are expected to follow NMC policies, best practices, and industry standards to avoid laptop theft and/or breach of NMC Confidential Information.

3.2.2.3.5. Security locks, alarms, or tracking devices will be appropriately used to physically secure Workstations in areas that are accessible to the general public. The User and department manager are jointly responsible for securing devices and ensuring compliance in coordination with the IT department.

3.2.2.4. Remote Access

3.2.2.4.1. Users accessing the NMC network or information from remote locations, such as connections from home, should employ appropriate security safeguards. For more information about remote access, please see the **NMC Remote Access** policy (Doc ID 867)

3.2.2.5. Personal Software

3.2.2.5.1. Installation of personal software, purchased or downloaded, including, but not limited to screensavers and animated GIFs, by employees is prohibited. Software required for end user purposes must be approved and installed by IT. Software installations will be coordinated through IT by calling 1113 or opening a Help Desk ticket.

3.2.2.6. Clearance

3.2.2.6.1. Employees, physicians, volunteers, and outside vendors are required to have appropriate clearance prior to access to computer workstations.

3.2.2.7. Removal

3.2.2.7.1. Upon termination or change of job position, users will have network access removed or modified.

3.2.3. Physical

3.2.3.1. Physical Placement and Monitoring

3.2.3.1.1. Physical Workstation placement should minimize the possibility of unauthorized personnel viewing screens or data.

3.2.3.1.2. Physical devices such as privacy guards will be utilized where needed to limit visibility of confidential information to unauthorized personnel.

3.2.3.1.3. Workstations in high traffic areas used to access confidential information will be monitored during business hours.

3.2.3.1.4. Department managers are ultimately responsible for the physical placement and monitoring of Workstations in their areas.

3.2.3.1.5. All workstations must be positioned or located in a manner that will minimize the exposure of any displayed patient or sensitive business information. When necessary, privacy screens should be deployed.

3.2.3.1.6. Workstations must be installed with physical safeguards to eliminate or minimize the possibility of unauthorized access to information or theft of equipment. To the extent possible, equipment should be located in areas that have some degree of physical separation from the public and, where possible, should face away from the public. Where computers cannot be protected from public view, privacy screens are mandated. When applicable, computer screens should also face away from other employees to ensure privacy of sensitive material.

3.2.3.1.7. Workstation equipment and portable computing devices will be protected from exposure to physical threats including theft based on potential risk and available safeguards.

3.2.4. Technical

3.2.4.1. All workstations must be equipped with security hardware and/or software. Where appropriate, all workstations and portable devices must be equipped with updated software for detecting the presence of malicious software (e.g. computer viruses). All computing devices must have current versions of anti-virus software enabled. Operating systems must have all critical updates installed.

3.2.4.2. Timeouts:

3.2.4.2.1. Screen Savers:

3.2.4.2.1.1. Screen savers on Workstations will be configured to automatically enable after five (5) minutes of inactivity. This protects PHI or Confidential Information from being inappropriately displayed should the User accidentally leave the Workstation without manually enabling the screen saver. The following screen saver controls should be in place:

- All Clinical workstations will be set to time out at five (5) minutes without a password lock.

- All Common workstations will be set to time out at five (5) minutes without a password lock.
- Any exceptions to the above policy will require a formal business waiver initiated by the business unit for the area represented and will require the approval of the NMC HIPAA Security Officer.

3.2.4.2.2. Auto Logoff:

3.2.4.2.2.1. All systems containing sensitive patient or business information will be enabled with auto log-off capabilities if available. The delay will be determined based upon the following risk criteria:

- number of users having access to the application,
- number of patient records (high numbers are higher risk),
- location (higher traffic or public would be high risk),
- level of sensitivity of the information (HIV, oncology, performance evaluations, etc.).

3.2.4.2.2.2. Workstations dedicated to supporting a specific application or information system are not required to be logged out of the specific application, logged out of the network at the end of the business day. These workstations must be documented by the Information Technology (IT) department.

3.3. Software Control:

3.3.1. Ensures that software on each workstation on the network is internally compatible and will not lead to degradation of the system.

3.3.1.1. Unauthorized changes to the desktop hardware, file structure, or system configuration are not allowed.

3.3.1.2. Application features are not to be disabled (e.g. virus software or auditing capabilities).

3.3.2. Users are not permitted to download, install, or save any unauthorized software or applications to the network or hard drives without prior approval from IT.

3.3.3. Software and Operating System Configuration

3.3.3.1. All workstations will be configured according to approved IT standards.

3.3.3.2. All workstations must be equipped with updated software for detecting the presence of malicious software (e.g., computer viruses). All computing devices must have current versions of anti-virus software enabled. Operating systems must have all critical updates installed.

3.3.4. Storing Documents and Files

3.3.4.1. Work-related documents, including NMC and PHI data, should be stored on appropriate network drives.

3.3.4.2. Data should not be stored on, transferred to, or transferred from, hard drives or removable media like zip drives, floppy drives, USB devices and diskettes unless there is a legitimate business purpose.

3.3.4.3. Only data stored on network drives is backed up and available for restoration in the event of data loss.

3.4. Mobile Control:

3.4.1. Establishes the security requirements for the appropriate use of mobile computing resources including laptops, tablets, and smart phones that access NMC information or connect to the NMC network

3.4.2. Portable Computing Devices

3.4.2.1. The loss or theft of any portable computing device on which NMC patient or sensitive business information is stored shall be immediately reported to Department Supervisor whether or not the hardware is owned by NMC. The supervisor will contact the NMC HIPAA Security Officer.

3.4.2.2. Startup authentication and authorization passwords (user name and password) are required on all portable-computing devices that store patient health information (PHI) or confidential data whether or not the hardware is owned by NMC. Additional passwords and/or encryption may be required at the discretion of the IT department.

3.4.2.3. Passwords and user IDs for computer systems and networks must not be stored on portable computing devices.

3.4.2.4. The IT department will establish approved remote access via portable computing devices, when necessary.

3.4.2.5. Portable computing devices that have stored data belonging to NMC may not be shared with others who are not authorized to access that information unless that information is stored as encrypted password protected files.

3.4.2.6. Vendors, consultants, business associates and all others wishing to connect portable computing devices to the NMC network must first submit the equipment to NMC IT for inspection of the adequacy of anti-virus software and installation of critical operation system updates. Contact the IT Help Desk at 1113 to initiate this process.

3.4.2.7. Users should contact the IT Help Desk (1113) for more information or assistance if they feel that their portable computing device contains particularly sensitive information requiring higher levels of protection.

3.4.2.8. NMC reserves the right to identify particularly sensitive information and initiate methods to secure such information.

3.4.3. All laptops and any other portable computer equipment must be secured (protected) when not in use. Proper security is dependent on risk factors and available resources at specific locations throughout NMC. Security may be provided by locking the equipment in a cabinet, desk, office, etc. Where such alternatives are not feasible, keeping the device out of sight in a desk or briefcase may be appropriate.

3.4.3.1. All laptops, tablets, and other mobile devices must be encrypted by NMC's enterprise encryption solution. Any exception must be documented by the IT department and appropriate compensating controls put into place.

3.4.3.2. Keeping information stored on a portable computing device secure and current is the responsibility of the person who has the device in his or her possession and control. Those in possession are responsible for breaches of security related to devices in their possession. The ability to write data to Portable Computing Devices such as USB drives is only permitted if the user has authorized our system to encrypt the device. Otherwise, one may only read data from the device.

3.5. User Education:

3.5.1. Ensures that users are oriented and trained on workstation use

3.5.2. Good judgment and reasonable care should be exercised to avoid damaging equipment (e.g. do not drop the device or spill liquids on equipment).

3.5.3. Ethical Workstation Use:

3.5.3.1. Appropriate use of resources includes maintaining the security of the system, protecting privacy, and conforming to applicable laws, including Copyright and harassment laws.

3.5.3.2. Workstations are to be used primarily for the conduct of NMC business.

3.5.3.3. Attempts to maliciously sabotage systems or networks using NMC resources are prohibited.

3.5.3.4. Attempts to make a computer impersonate other systems, particularly via forged email, talk, news, etc., are prohibited.

3.5.3.5. Users may not use their accounts to attempt to gain unauthorized Access to NMC or non-NMC systems.

3.5.3.6. Unless the information system is unavailable for maintenance or there is a specified business reason preventing routine User Access, NMC users may not deliberately deny authorized Users Access to systems.

3.5.3.7. Users are not to interfere with or alter the integrity of the information system at large by destruction or unauthorized alteration of data or programs belonging to other Users.

3.5.4. Computer access and password training, provided by the IT department, must be completed before access privileges are granted to ensure adequate training has occurred.

3.5.5. Keep food and drink away from workstations in order to avoid accidental spills.

3.5.6. NMC Community Members should ensure workstations are left powered on, but logged off in order to facilitate after hours updates.

3.5.7. Exit running applications and close open documents when leaving workstation unattended.

3.5.8. Users are required to log-off of applications containing patient health or sensitive business information before leaving their workstations.

3.5.9. Users are strongly encouraged to save work to the network. When the user does not use the NMC network to store information and instead, uses other media, e.g. hard drive, diskettes, usb drives, etc, it is the responsibility of the user to make back-up copies of such information on a frequent basis. For assistance, contact the IT Help Desk at 1113.

3.5.10. In the event a critical document or file is inadvertently deleted, contact the IT Help Desk at 1113. Do not continue to use the workstation, or save additional work.

3.6. HIPAA Requirements

3.6.1. Ensure the requirements of the HIPAA Security Rule “Workstation Security” Standard 164.310(c) are met.

3.6.2. Policy Violations and Sanctions:

3.6.2.1. Violations of this policy will be processed according to applicable NMC policies, including the NMC Progressive Corrective Action Policy, as well as civil and criminal laws.

3.6.2.2. Non-compliance with this policy is subject to management review and action, up to and including termination of employment, vendor contract and/or legal action.

3.6.2.3. Any Workforce member who observes a person violating this policy will promptly notify his or her supervisor, a representative of Human Resources, or the NMC Corporate Compliance Office at 800-633-6399. Workforce members who violate this policy may be subject to corrective action, including involuntary separation.

4.0. REFERENCES

4.1. HIPAA Security Rule “Workstation Security” Standard 164.310(b)

4.2. HIPAA Security Rule “Workstation Security” Standard 164.310(c)