1.0. Purpose:
- 1.1. To ensure authorized users are granted the level of access to information and data appropriate to their job assignments or functions and unauthorized users are prevented from accessing any data. Assigning a unique name and/or number allows the system administrator to be able to identify and track users on the system.
- 1.2. To mitigate the risk an unauthorized user may use an authorized user's account after the authorized user has logged in.

2.0 Policy:
- 2.1 This policy outlines how a user must have unique authentication in place in order to access Newton Medical Center's Electronic Protected Health Information (EPHI).

3.0 Definitions:
- 3.1 EPHI Repository: A database, spreadsheet, folder, storage device, document or other form of electronic information that is accessed by one or more users.
- 3.2 Legacy system: An existing or old computer system used to support a specific program area. The term is used generically to distinguish the existing or old system from the new or planned system.

4.0 Procedure/Guidelines:
- 4.1 Unique User Identification and Password
  - 4.1.1 To uniquely identify and track each user for the purpose of access control to all networks, systems, and applications that contain EPHI, and the monitoring of access to the aforementioned networks, systems, and applications each department must comply with the measures outlined in this Policy.
  - 4.1.2 Any user that requires access to any network, system, or application that access, transmits, receives, or stores EPHI, must be provided with a unique login credentials.
  - 4.1.3 When requesting access to any network, system, or application that accesses, transmits, receives, or stores EPHI, a user or workforce member must supply their previously assigned unique user identification in conjunction with a secure password to gain access to the aforementioned networks, systems, or applications.
  - 4.1.4 Users or workforce members should:
    - 4.1.4.1 Not allow another user or workforce member to use their unique user identification or password.
    - 4.1.4.2 Ensure that their user identification is not documented written, or otherwise exposed to an insecure manner.
    - 4.1.4.3 Ensure that their assigned login/password is appropriately protected and only used for legitimate access to networks, systems, or applications.
    - 4.1.4.4 If a user believes their user identification has been compromised, they must report that security incident to their manager, who will contact the appropriate HIPAA Officer.

4.1.5 The use of a common or shared User IDs and password is not permitted. The following exceptions can be discussed with the HIPAA Security Officer if the following conditions have been met:

- 4.1.5.1 A screen saver or workstation login located in a shared environment such as a nurse's station or procedure room.
- 4.1.5.2 Physical access to the workstation by unauthorized personnel can be controlled.
- 4.1.5.3 The workstation login must not provide access to applications or databases containing medium or high risk EPHI.
- 4.1.5.4 A user's access to EPHI can still be logged and audited based on their unique identification.
- 4.1.5.5 All such requests must be submitted to the HIPAA Security Officer or must contain (1) detailed business case explaining why individual logins will not suffice and (2) signature of the requesting areas Director and VP.

4.1.6 Each user's password must meet the following minimum requirements:

- 4.1.6.1 Passwords must be a not less than eight characters in length.
- 4.1.6.2 Incorporate a combination of three of the following characteristics:
  - 4.1.6.2.1 Any lower case letters (a-z)
  - 4.1.6.2.2 Any upper case letters (A-Z)
  - 4.1.6.2.3 Any numbers (0-9)
  - 4.1.6.2.4 Any punctuation or non-alphanumeric characters found on a standard ASCII keyboard (! @ # $ % ^ & * ( ) _ - + = { } [ ] : ; " ' | \ / ? < > , . ~ `)
- 4.1.6.3 Password must not contain three or more consecutive characters from the user's account name or display name. (This check is not performed for account names with fewer than 3 characters).
- 4.1.6.4 Passwords should not include easily guessed information such as personal information, names, pets, birth dates, etc.
- 4.1.6.5 Passwords should not be words found in a Dictionary.
- 4.1.6.6 The previous 4 passwords used are not available for reuse.
- 4.1.6.7 Passwords automatically expire after 180 days or 6 months.

4.1.7 If a system does not support the minimum structure and complexity as detailed in the aforementioned guidelines, one of the following procedures must be implemented:

- 4.1.7.1 The password assigned must be adequately complex to ensure that it is not easily guessed and the complexity of the chosen alternative must be defined and documented.
- 4.1.7.2 The legacy system must be upgraded to support the requirements as soon as administratively possible.
- 4.1.7.3 All EPHI must be removed and relocated to a system that supports the foregoing security password structure.

4.2 Automatic Logoff

4.2.1 To ensure access to all servers and workstations that access, transmit, receive, or store EPHI is appropriately controlled, the following must be followed:

4.2.1.1 Servers, workstations, or other computer systems containing EPHI repositories that have been classified as high risk must employ inactivity timers or automatic logoff mechanism. The aforementioned systems must terminate a user session after a maximum of 15 minutes of inactivity.

4.2.1.2 Servers, workstations, or other computer systems located in open, common, or otherwise insecure areas, that access, transmit receive, or store EPHI must employ inactivity timers or automatic logoff mechanisms.

4.2.1.3 Applications and databases using EPHI, such as electronic claims records, must employ inactivity timers or automatic session shutoff mechanisms. The aforementioned application sessions must automatically terminate after a maximum of 15 minutes of inactivity.

4.2.1.4 Servers, workstations, or other computer systems that access, transmit, receive, or store EPHI, and are located in locked or secure environments need not implement inactivity timers or automatic logoff mechanisms.

4.2.1.5 If a system that otherwise would require the use of an inactivity timer or automatic logoff mechanism does not support an inactivity timer or automatic logoff mechanism, one of the following must be implemented:

4.2.1.5.1 The system must be upgraded or moved to support the required in activity timer or automatic logoff mechanism.

4.2.1.5.2 The system must be moved into a secure environment.

4.2.1.5.3 All EPHI must be removed and relocated to a system that supports the required inactivity timer or automatic logoff mechanism.

4.2.1.6 When leaving a server, workstation, or other computer system unattended, users must lock or activate the systems logoff mechanism or logout of all applications and database systems containing EPHI.

4.3 Firewall Use

4.3.1 All networks housing EPHI repositories must be appropriately secured. To ensure all networks that contain EPHI-based systems and applications are appropriately secured, the following must be followed:

4.3.1.1 Networks containing EPHI-based systems and applications must implement perimeter security and access control with a firewall.

4.3.1.2 Firewalls must be configured to support the following minimum requirements:

4.3.1.2.1 Limit network access to only authorized workforce members and entities.

4.3.1.2.2 Limit network access to only legitimate or established connections. An established connection is return traffic in response to an application request submitted from within the secure network.

4.3.1.2.3 NMC must document its configuration of firewalls used to protect networks containing EPHI-based systems and applications. This documentation should include a configuration plan that outlines and explains the firewall rules.

4.4 Encryption

4.4.1 Encryption of EPHI as on access control mechanism is not required unless the custodian of said EPHI deems the data to be highly critical or sensitive.

4.4.2 Encryption of EPHI is required in some instances ass a transmission control and integrity mechanism. However, encryption of the following devices in NMC is required:

4.4.2.1 PCs

4.4.2.2 Laptops, tablets

4.4.2.3 Flash drives, thumb drives

4.4.2.4 All the aforementioned devices must be encrypted using the Dell Enterprise Encryption (DEE) solution.

4.5 Wireless Access

4.5.1 To ensure all networks containing EPHI-based systems and applications are appropriately secured, the following security measures must be followed:

4.5.1.1 Encryption must be enabled.

4.5.1.2 MAC-based or User ID/Password authentication must be enabled.

4.5.1.3 All console and other management interfaces have been appropriately secured or disabled.

4.5.1.4 Unmanaged, ad-hoc, or rogue wireless access points are not permitted on any secure network containing EPHI-based systems and applications.

4.6 External Entities

4.6.1 Access to confidential locations (i.e.; Generations) is not granted to outside entities.

4.6.2 Access will be limited to each user's specific provider group.

4.7 Remote Access

4.7.1 Dialup Connections directly into secure networks or secure systems are considered to be secure connections and do not require a VPN connection. This implementation of secure remote access extends the secure network to the remote user using a secure Public Switched Telephone Network (PSTN) connection.

4.7.2 Authentication and encryption mechanisms are required for all remote access sessions to networks containing EPHI via an Internet Service Provider (ISP)

or dialup connection. Examples of each mechanisms include VPN clients, authenticated SSL web sessions, and Sun secured desktop client access.

4.7.3 All encryption mechanisms implemented to comply with this policy must support a minimum of, but not limited to, 128-bit encryption.