NYGH POLICY & PROCEDURE NUMBER: V-75

SUBJECT: **MOBILE DEVICES, REMOVABLE STORAGE MEDIA & PERSONAL HEALTH INFORMATION SECURITY**

CROSS REFERENCE: E-mail Policy: X-15

APPROVED BY:

DATE ISSUED: March 2008
DATE REVIEWED:
DATE REVISED:

AUTHORIZATION:

GUIDING PRINCIPLES

North York General Hospital (NYGH) protects its information assets and personal health information by using physical, technical and administrative safeguards and by not permitting storage of personal health information on mobile devices or removable storage media except in encrypted form.

Employees, whether contract or permanent, and physicians will be held accountable for the physical security of mobile devices and removable storage media and for protecting the confidentiality of personal health information.

This policy responds to s.10 and s.12 (1) of the *Personal Health Information Protection Act* and to principles of Accountability and Safeguards.

INTERPRETATION

Personal health information means oral or recorded information about an identifiable individual that relates to:

a) their physical or mental health including the family health history;

b) provision of health care to the individual including identifying a person as the individual's health care provider;

c) is a plan of service for the individual within the meaning the Long-Term Care Act, 1994;

d) payments or eligibility for health care in respect of the individual;

e) an individual's donation of any bodily part or bodily substance or is derived from testing a body part or substance;

f) is the individual's health number

g) identifies an individual's substitute decision maker

Mobile devices include laptop computers, personal digital assistants (Blackberries & similar), MP3 players, iPods, iphones and emerging technologies that may be used to store personal health information (not an exhaustive list).

Removable storage media include a USB key (Compact Flash, SmartMedia), magnetic hard disk, magnetic tape, CD-ROM, DVD, magnetic optical disk, floppy disk/zip disk (not an exhaustive list).

POLICY:

1. Advanced Encryption Standard 256 (AES-256) whole disk encryption software must be installed on all NYGH laptop computers.

2. Personal health information (PHI) may only be stored on a laptop where AES-256 whole disk encryption software has been installed and enabled. The software must be reviewed and updated as necessary.

3. Laptop computers not owned by NYGH may connect to the Internet through the guest Virtual Local Area Network.

4. Laptops must have anti-virus and anti-spy ware programs installed and enabled and they must be regularly updated with the appropriate security patches.

5. Desktop and laptop computers will be configured to ensure that information may only be copied to removable media in AES-256 encrypted form.

   5.1 The software will permit desktop and laptop computers to read unencrypted information stored on removable media.

6. Personal health information (PHI) must not be stored on the following mobile devices: personal digital assistant, MP3 player, iPod, iphone or similar emerging technology capable of storing PHI.

7. Audit logs will be maintained of all files copied to mobile devices and removable media.

8. Mobile devices and removable storage media must be identifiable as the property of NYGH to facilitate recovery if lost or stolen.

9. The NYGH virtual private network, the secure remote access protocol and the Smart Systems for Health Agency's (SSHA) ONE Network and ONE Mail provide a high level of protection for PHI therefore these systems must be used for transmission and access where feasible.

   9.1 The NYGH e-mail system provides secure transmission of PHI and confidential information between NYGH sites. Information is

protected during transmission to all NYGH e-mail addresses i.e. from sendername@nygh.on.ca to receivername@nygh.on.ca.

9.2 The NYGH e-mail system also permits PHI to be securely transmitted to registered SSHA ONE Mail users. SSHA One Pages is a searchable listing of health care providers who are registered users of ONE Mail. Before transmitting PHI, check ONE Pages to ensure that the intended recipient is a registered user of ONE Mail. Do not transmit PHI if the intended recipient is not listed on ONE Pages.

9.3 The Ontario Telemedicine Network relies on SSHA technology systems and similarly provides for secure transmission of PHI.

A: PASSWORDS

1. Strong login passwords must be used on desktops, mobile devices and removable storage media that contain a combination of letters, numbers and symbols, a minimum of eight characters and no dictionary words.

1.1 Passwords must not be shared, written down or stored on a desktops, mobile devices or removable storage media.

1.2 The password-locking feature of a desktop/laptop computer screensaver must be used when the computer is unattended for brief periods except as set out in 1.3.

1.3 The mobile computers on carts used by physicians and nurses must have the screensaver enabled during rounds. The password-locking feature must be used when it will not cause disruption to care or if unattended for other than a brief period.

1.4 Turn off laptop computers if they will be unattended for more than brief periods unless they are in a secure location such as a locked office.

1.5 Two factor authentication must be installed and enabled on mobile devices where the Director, Information Services determines it technically feasible and warranted.

1.6 Personal digital assistants (PDAs) will be configured to destroy information and to revert to factory settings following 10 unsuccessful log-in attempts.

B: SECURE STORAGE

1. Mobile devices and removable storage media must be stored securely when not in use.

1.2 Secure storage means a locked office, locked drawer, locked filing cabinet or locking cable. Use a combination of methods to further strengthen security where possible.

C: LAPTOP COMPUTERS

1. Laptops must have AES-256 whole disk encryption installed and enabled before PHI may be stored on them.

2. The PHI must be limited to that necessary to perform employment duties and be made anonymous where feasible.

3. Ensure that files are only being copied to the laptop and not moved.

4. A list must be kept of files containing PHI that are stored on a laptop.

   4.1 The list must be updated regularly and be maintained separate from the laptop together with the make, model and serial number.

5. After completion of work on files containing PHI, they must be uploaded to the network and then deleted from the laptop.

D: PERSONAL DIGITAL ASSISTANTS (PDAs)

1. For PDA's that rely on Bluetooth or similar technology, the default position for Bluetooth should be "off", and the PDA set to "non-discoverable".

2. Never simultaneously connect to Wi-Fi and Bluetooth. Doing so would create an open bridge or access point, a serious security risk.

SUBJECT: **MOBILE DEVICES, REMOVABLE STORAGE MEDIA & PERSONAL HEALTH INFORMATION SECURITY**

CROSS REFERENCE: E-mail Policy: X-15

APPROVED BY:

DATE ISSUED: March 2008
DATE REVIEWED:
DATE REVISED:

AUTHORIZATION:

E: REMOVABLE STORAGE MEDIA

1. PHI may only be copied to removable storage media in AES-256 encrypted form.

    1.1 Ensure the PHI is only copied and not moved to the removable media.

2. Strong login passwords must be used on the removable media that contain a combination of letters, numbers and symbols, a minimum of eight characters and no dictionary words.

    2.1 Passwords must not be shared, written down or stored on computers or the removable media.

    2.2 The password must not be the same as one used to log in to your computer or other mobile device.

    2.3 A list of files should be maintained of PHI stored on removable media.

3. Never leave removable media unattended in a computer and store it securely when not in use.

4. Delete the PHI from removable media as soon as it is no longer needed.

SUBJECT: **MOBILE DEVICES, REMOVABLE STORAGE MEDIA & PERSONAL HEALTH INFORMATION SECURITY**

CROSS REFERENCE: E-mail Policy: X-15

APPROVED BY:

DATE ISSUED: March 2008
DATE REVIEWED:
DATE REVISED:

AUTHORIZATION:

F: WORKING OFFSITE

1. PHI may only be stored on a laptop or removable storage media for the purpose of working outside of the hospital when the information cannot be remotely accessed through a secure website or the NYGH virtual private network.

2. Files containing PHI must be backed up to the network before traveling with a laptop or removable media.

3. Mobile devices and removable storage media must be kept with you at all times when working outside of the hospital if secure locked storage is not available.

4. Laptop computers must be turned off when not in use to protect against retrieval of passwords and encryption keys from temporary memory.

5. If a mobile device or removable storage media must be left in a vehicle, lock it in the trunk at the start of the trip and not at the destination.

6. Never leave mobile devices or removable storage media in a vehicle overnight.

7. The default position for laptop Wi-Fi access must be set to "off" when working outside the hospital on files containing PHI.

SUBJECT: **MOBILE DEVICES, REMOVABLE STORAGE MEDIA & PERSONAL HEALTH INFORMATION SECURITY**

CROSS REFERENCE: E-mail Policy: X-15

APPROVED BY:

DATE ISSUED: March 2008
DATE REVIEWED:
DATE REVISED:

AUTHORIZATION:

G: THEFT, LOSS AND OTHER HARMS

1. If a mobile device or removable storage media is stolen or lost or there has been unauthorized access, use, disclosure, modification or destruction of PHI, immediately notify the Chief Privacy Officer at 416-756-6448 and Security at 416-756-6408.

    1.1 Provide Security and the Chief Privacy Officer with the list of files stored on the mobile device or removable storage media and the make, model and serial number of the mobile device.