Halton Healthcare GEORGETOWN · MILTON · OAKVILLE	**Use of Technology Policy**			
	Program/Dept:	Information and Communication Technology	Document Category:	Info & Comm Tech
	Developed by:	Information and Communication Technology	Original Approval Date:	Oct. 2004
	Approved by:	Senior leadership team and Medical advisory committee	Reviewed Date:	November 2018
	Review Frequency:	1 year	Revised Date:	November 2018

Information and Communication Technology Use of Technology Policy Contents

Policy

Halton Healthcare's information technology includes all hardware and software used to capture, store, retrieve, access, and for distribution of information. This includes, but is not limited to: computers, laptops, tablets, printers, scanners, photocopiers, facsimile machines, cell phones, smart phones, card access devices, telephone systems, servers, e-mail service, network and remote access infrastructure. These resources are made available to staff, volunteers, physicians and affiliates in support of their job functions.

This policy sets out principles, guidelines, rules and specific procedures that are to be followed when using Halton Healthcare information technology. The security and integrity of Halton Healthcare information and information technology is maintained through a combination of security technology, policies, training and adherence to these policies by users.

All users of Halton Healthcare information technology are expected to be familiar with this policy, and failure to adhere to this policy may result in loss of access privileges and/or other disciplinary measures up to and including termination.

Procedure

1.1 Access to Technology

All access to technology at Halton Healthcare will be coordinated by Information and Communication Technology (henceforth 'ICT'). Access to the technology at Halton Healthcare will be restricted to those who require it as part of their job function. Specific requests for access must be forwarded to ICT by the responsible manager, supervisor or director. The delegation of system administrative duties are evaluated and approved by ICT on a case-by-case basis.

Human Resources uses the 'HR Notification' web form to notify ICT of all new hires. User names and access are granted by the ICT department. If a new user fits within an identified category/group, they will be assigned the same access as their counterparts.

Access is activated after the users have received the training determined to be necessary by their department, have attended a regular hospital orientation session and have signed the appropriate agreements as follows:

User Type	Agreement	Managed By
Staff	Confidentiality Policy	Human Resources
Students/Volunteers	Confidentiality Policy	Human Resources/ICT
Physicians	Computer Access Agreement – Physicians	Medical Staff Office
External Agents	Confidentiality Policy for External Agents	Clinical Information Services
	3rd Party Remote Access Agreement	ICT
	Business Associate Agreement	ICT

In addition, it is acknowledged that Physicians are governed by the College of Physicians and Surgeons of Ontario [Medical Records #11-00, Confidentiality and Access to Patient Information #9-00] Regulated Healthcare Professionals are governed by their respective colleges.

Human Resources uses the 'HR Notification' web form to notify ICT of all staff who have been terminated or who have retired. ICT inactivates the user's account in the computer system effectively terminating access to the system.

1.2 Privacy and Confidentiality

All Halton Healthcare staff using information technology are responsible for adhering to Halton Healthcare privacy and confidentiality policies and procedures (refer to Confidentiality Policy and Personal Health Information and Privacy Policy). Halton Healthcare staff are also required to successfully complete the Privacy and Security e-learning module on an annual basis.

1.3 Intended Use

1.3.1 Acceptable Use

Halton Healthcare is committed to fostering a work environment in which all persons are treated with dignity and respect. Accordingly, Halton Healthcare information technology **cannot** be used to create, store or distribute:

- Material that contains offensive or discriminatory content about age, race, religion, creed, gender, sexual orientation, political beliefs, language, disability or national origin.
- Material of a malicious or threatening nature.
- Material that is sexually explicit or may be considered vulgar or obscene.
- Material that violates provincial or federal laws, professional codes of ethics, or any Halton Healthcare policy.
- Material that, by volume alone, will compromise system resources.
- Material that includes personal business ads, solicitations, promotions or commercial announcements without prior approval from an employee's respective manager.
- Photography and audio/video recording must follow procedures identified in the "Photography/Videography Electronic Recording on Halton Healthcare Property Policy".

1.3.2 Personal Use

Information Technology systems may be used for occasional or incidental personal use under the following conditions:

- Personal use must not interfere with job functions
- Personal use must not interfere with the normal operation of underlying technology (e.g. Bandwidth)
- Personal use is prohibited where it results in direct costs to Halton Healthcare (i.e. long distance phone calls) without explicit approval from an employee's respective manager
- Personal use is subject to, and must conform with, all Halton Healthcare policies.

1.4 Security

All users of information technology share a responsibility for protecting equipment and information from unauthorized access, loss, corruption, theft or destruction:

- All equipment should be kept physically secure and surrounding enclosures and doors locked when equipment is left unattended.
- Equipment should be placed in such a way as to prevent PHI and Personal Information from being observed by unauthorized persons.
- Users must log out/off systems to prevent others from accessing the system under their authentication parameters (usernames and passwords)Screen savers with passwords should be used in circumstances where logging off is not practical and where locked enclosures are not available.
- Laptop computers and other portable devices such as, but not limited to, smartphones and tablets that contain PHI and Personal Information must be encrypted to prevent unauthorized access in the event of theft.
- Installation of software (via internet or electronic media) on any of Halton Healthcare information technology equipment is strictly prohibited. (section 1.9 below)

- All Microsoft Windows systems have a local Administrator account which has elevated privileges (super user) access, and is commonly used by malicious attackers to attempt to compromise systems. For most staff administrative permissions are not required to perform day to day activities. Halton Healthcare staff are automatically provided with access rights on their machine that do not include administrative permissions. If administrative permissions are required, staff should contact the ICT Team to schedule time to provide these permissions. Permanent exceptions may be granted as needed by the ICT department to Halton Healthcare staff who require administrator permissions to perform job related tasks.

Users who attempt to change security settings, circumvent, or without authorization, disclose to a third party the hospital's internal security policies, procedures or practices, are subject to disciplinary action as outlined under "Policy" above. Any exceptions relating to Security must be approved by the ICT Director.

1.5 Auditing and Auditing Process

For purposes of this policy, an audit is the process of comparing actual use of an information resource against the identified policies, processes, standards and procedures governing the use of the resource. Security and Privacy Audits are manually, automatically and/or systematically conducted to ensure integrity, confidentiality and availability of information and resources.

Audits will remain objective and systems will only be audited against their intended use. ICT maintains a Service Catalog that identifies all Halton Healthcare Systems and the intended use of that system. The Application owner (with ICT support) is responsible to review the workforce members that have access to their systems on a regular basis and ensure regular auditing is performed on their systems. The sensitivity of the system will determine the type of auditing that must be performed. (E.g. The Meditech System will have a different audit scope and frequency than the Food Services System)

Halton Healthcare reserves the right to audit systems outside their intended use to support employee investigations and where there is probable cause of conduct outside of acceptable use as defined in Section 1.3.1 or any other Halton Healthcare policy. Senior Management must approve an audit and the release of the audit results.

For physicians, Halton Healthcare reserves the right to audit systems outside their intended use where there is probable cause of conduct outside of acceptable use as defined in Section 1.3.1 or any other Halton Healthcare policy. The Chief of Staff must approve an audit and the release of the audit results.

1.6 Usernames and Passwords

Access to many of the information and communications systems in use at Halton Healthcare requires individual authentication parameters (user codes, passwords) which define the user's access privileges and ensure unauthorized parties cannot access the systems.

- Individual authentication parameters belong exclusively to the user to whom they are assigned and should never be shared with others.
- When used in software applications the individual authentication user name is equivalent to an individual's signature.
- All users assigned individual authentication parameters are responsible for taking the necessary precautions to ensure they are not revealed.

- Users are responsible for all activity that occurs under their unique parameters. Users who suspect that their authentication parameters may be known by others must immediately arrange to have them changed with the ICT department. (x7777). ICT reserves the right to suspend user access or use of access parameters based on credible evidence these credentials may have been shared and/or obtained by an external party through illicit or intentional means
- It is a breach of Halton Healthcare Policy to reveal your authentication parameters, as well as to knowingly use the access parameters of another user or to knowingly impersonate another user in any way.
- ICT staff can only grant access to employees or contractors under the direction of the user's supervisor. ICT staff (or delegated system administrators) are responsible for ensuring that all access is properly authorized, and that all required policies have been reviewed (and signed/filed if necessary) prior to granting access.
- Selecting a safe password and ensuring it is not revealed is a very important component of the Halton Healthcare overall security framework. Passwords are never displayed when entered, but users should ensure when they authenticate that their keystrokes cannot be observed by others.
- Passwords should be selected in order to prevent the need to record them in writing and should not be easily guessed by others (i.e. you or a significant other's birth date, nicknames etc.).
- All passwords should be complex enough that it would be impractical for an attacker to guess or otherwise discover the correct secret value. A combination of alphabetic, numeric and special characters is recommended. Names and dictionary words alone should not be used (i.e. use dictionary words only in conjunction with other methods/factors). A recommended approach is to start with something that is known to you, but would be difficult to determine by others (the street you grew up on) and add a digit or special character (substitute "$" for an "s").

1.7 Internet Use

The Internet is an important resource for staff and physicians working at Halton Healthcare. Internet resources include, but are not limited to access to the World Wide Web, FTP (file transfer protocol) servers, the Intranet, and Halton Healthcare domain names and IP addresses, including all Halton Healthcare networks in which Internet is available. Halton Healthcare uses filtering technology to prevent access to sites that contain offensive material and malicious content; however this filtering prevents most but not all threats. For this reason, Halton Healthcare must also rely on the professional behaviour of staff and physicians to protect its systems. In addition, for purposes of clinical care and/or education, there may be exceptions where websites or videos that may be deemed inappropriate are accessed. Internet use at Halton Healthcare shall comply with all Federal and Provincial laws, and will not violate other sections in this policy or any Halton Healthcare policy. The internet cannot be used to transmit PHI and Personal Information unless it is first encrypted using a method authorized by ICT. Internet mail can only be used to communicate with patients if it complies with the organization's privacy policies and principles.
Inappropriate Internet use includes, but is not limited to:

- Software or files from the internet must never be downloaded or installed without prior approval of Information and Communication Technology. For example when using the internet, if users are presented with a question asking if they would like to "download", "install" or "update" something, they should always answer no.
- In order to prevent damage to its systems, the hospital prohibits the transmission, receipt or creation of files that may contain viruses and users must exercise extreme caution when using the internet.
- Usage for illegal purposes, such as theft, fraud, slander, libel, defamation of character, harassment (sexual and non-sexual), stalking, identity theft, online gambling, spreading viruses, spamming, impersonation,

intimidation, and plagiarism/copyright infringement.

- Any usage that conflicts with existing Halton Healthcare policies and/or any usage that conflicts with Halton Healthcare mission, goals, and reputation.
- Access to internet sites that distribute files or software (file sharing sites) prohibited at Halton Healthcare unless pre-approved by the ICT department.
- Access to video streaming sites is prohibited at Halton Healthcare unless pre-approved by management and the ICT department.
- Copying, destroying, and altering any data, documentation, or other information that belongs to Halton Healthcare or any other business entity without authorization.
- Accessing, viewing, downloading, or printing any pornographic, threatening, harmful, abusive, harassing, defamatory, libelous, vulgar, obscene, hateful, or other objectionable content
- Engaging in personal online commercial activities, including offering services or products for sale or soliciting services or products from online providers.
- Allowing unauthorized or third parties to access Halton Healthcare network and resources.

1.7.1 Social Media

Refer to the corporate Social Media policy

1.8 E-mail

1.8.1 Internal E-mail

Halton Healthcare uses an e-mail system (Microsoft Exchange) for communication within the organization. Names listed in the Global Address List (GAL) are persons who can send/receive internal e-mail. Messages sent using the recipients in the GAL or with an e-mail address that contains @haltonhealthcare.on.ca or @haltonhealthcare.com using the mail system (Outlook or OWA from a Halton Healthcare computer) are considered secure.

Using the internal mail system to transmit PHI and Personal Information about patients should be done with care and the recipient list (at the “To:” prompt) should be double-checked to ensure only intended recipients within the organization are listed.

1.8.2 External Mail (Internet mail. E.g. Hotmail, Gmail)

Halton Healthcare’s E-mail system is connected to the internet, allowing users to send and receive messages to parties outside of the Halton Healthcare network (addresses not listed in the GAL or without @haltonhealthcare.on.ca). Internet mail is not secure and once a message is sent outside of the Halton Healthcare network it is in the public domain, and should be considered readable by anyone. Accordingly, internet mail cannot be used to send/receive PHI and Personal Information to external/non-One-Pages addresses. As internet mail is also the principal route for virus infiltration to Halton Healthcare network, extreme caution must be used when opening internet mail and attachments.

1.8.3 eHealth Ontario ONE Mail

ONE Mail is an e-mail transport service provided by eHealth Ontario that lets registered healthcare professionals communicate and share patient information quickly, confidentially and securely. Please contact the ICT department to configure the ONE Pages e-mail directory and provide a training session on the use of this technology.

1.8.4 Delegate Access to Halton Healthcare e-mail

The Halton Healthcare e-mail system allows users to have delegates access and manage their e-mail mailboxes. (E.g. administrative assistants may be delegates to a manager) Delegate access is required to be configured by the "owner" of the mailbox. When it is determined a delegate is required to access a mailbox, it is mandatory that delegates do not have access to any e-mail message marked as private. (Configured by default do not change) Halton Healthcare is using the private e-mail settings for technology solutions such as electronic signatures that must only be managed by the e-mail mailbox owner.

1.8.5 Forwarding Mail

Auto-forwarding should never be used to route mail to an external address and is forbidden under the participation agreement for eHealth Ontario's OneMail system.

1.8.6 Sending Messages to "All Users" and other distribution lists

When using distribution lists, users must ensure the selected list is appropriate and does not include a wider audience than is necessary for the type of message being sent. Distribution lists should not be used to convey sensitive or PHI and Personal Information. For assistance in creating personal distribution lists, or to create or alter global distribution lists, please contact ICT.

1.8.7 Virus Precautions

All external mail arriving at Halton Healthcare is scanned for viruses before it is forwarded to a user's inbox. As new viruses and threats emerge frequently, ICT shall regularly update hospital-owned/operated scanning systems in an attempt to detect and prevent threats from reaching users. Despite multiple protections, it is possible that an infected e-mail will reach a user without detection. Users play an important role in the Halton Healthcare virus prevention strategy and must ensure they use the mail system in a responsible way. Unsolicited e-mails received from unknown sources should not be opened or read and should be immediately deleted.

Unsolicited e-mail from known sources should also be treated with caution, and attachments should not be opened before investigating with the sending party. Many viruses now propagate by using the infected users address list. As such, even e-mail you receive from known or trusted parties may be infected. If you did not pre-arrange to receive an attachment from a known or trusted source, do not open the attachment.

1.8.8 Out-of-Office Assistant

This feature automatically replies to a message with a user-defined notice of absence. Users are encouraged to use this feature to indicate their absence when they will be away from work for a prolonged period of time. Caution should be taken when configuring Out of Office Assistance for people outside the organization. Configuring this option to send out of office messages to anyone outside the organization is a method used by "spammers" to confirm that an e-mail account is active and may cause an increase in spam to the e-mail account. Setting the external option to only send Out of Office replies to people listed in your Contacts is the preferred option.

1.8.9 Disclaimer

A disclaimer is automatically applied on all external emails sent from the Halton Healthcare e-mail system that reflects the hospital's privacy statement as well as expectations in the result of transmissions sent in error or to the wrong recipient.

1.9 Installation of Equipment/Devices/Software

In addition to existing operating and capital budget approval processes, Signing Authority Policy and Competitive Procurement Policy, the following will apply to the Purchase and Installation of Software, Equipment or Devices.

- The purpose and intended use for the equipment shall be identified including the location of the equipment, all software programs to be used on the equipment and the parties who will be using them.
- All purchases of ICT equipment/devices will be reviewed by Information and Communication Technology to ensure compliance with technical standards and consistency and appropriateness.
- A hardware configuration will be specified which includes the manufacturer, make and model of all components including processor, memory, hard disk, graphics, network interface card, monitor, keyboard, operating system that is in-line with current Information and Communication Technology standards. Variations from the standard shall require approval from the Director of Information and Communication Technology.
- Upon acquisition of hardware, ICT must configure the equipment to work at Halton Healthcare and ensure that the equipment is properly catalogued in the Information and Communication Technology inventory. All service performed on the equipment after installation is to be coordinated with ICT.
- Software License Agreements should be kept with the application owner or ICT as proof of purchase for all application software purchased.
- Software License Agreements and Software Copyright Law must be adhered to at all times on all ICT equipment in use at the hospital.
- All purchases of application software (including contracted programming) will be reviewed by ICT or Health Informatics Steering Committee to ensure appropriateness and that the necessary protections are sought and obtained.
- Only purchased software or software available for free commercial use will be installed and used on ICT equipment.

1.10 Personal Equipment and Home Use

Computers, Laptops, Tablets, Cell Phones and other personal devices that are not managed by ICT, cannot be connected to the primary Halton Healthcare network (with the exception of the ‘BYOD’ wireless network) without prior review and approval by ICT. Once approved and connected, the use of all non-Halton Healthcare equipment on the primary Halton Healthcare network is subject, but not limited to this and any related policies. Similarly, users connecting to the Halton Healthcare network from home or other off-site locations must abide by the elements of this, and any related policies.

Users of non-Halton Healthcare devices must take all reasonable precautions to safeguard the security and confidentiality of their remote access authentication parameters and any Halton Healthcare data that may be accessed with their equipment.

Users of non-Halton Healthcare devices (e.g. cell phones, tablets) acknowledge that Halton Healthcare will enforce and automatically deploy security settings to devices including but not limited to encryption, automatic screen lockout with password requirement, remote wiping capability and automatic wiping of the device if the wrong password is repeatedly entered. As a condition of synchronizing personal devices with the Halton Healthcare computing environment, users of non-Halton Healthcare devices understand that they are subject to the aforementioned security settings and restrictions.

Users of non-Halton Healthcare devices understand that if they do not make appropriate backups of any personal information maintained on their personal device, should the device be lost or stolen, personal information may be lost and is not the responsibility of Halton Healthcare.

Users of non-Halton Healthcare devices agree not to backup Halton Healthcare information (e.g., Business Sensitive Information (BSI) or Protected Health Information (PHI)) or move Halton Healthcare information from its encrypted area to any other unencrypted device. Home users understand their Halton Healthcare email mailbox information is maintained and backed up by Halton Healthcare and should not be replicated onto non-Halton Healthcare devices. Any exceptions must be approved by the ICT department.

Users of non-Halton Healthcare devices understand that modifying the underlying operating system of the device (e.g., "rooting", "Jailbreak-ing", etc.) will result in the device being removed from synchronization with Halton Healthcare data and. Users of non-Halton Healthcare devices agree further that they will not attempt to alter the operating system on the device and that if they encounter any evidence the operating system has been altered or controls removed by any means, (password is no longer required, account information is missing) they will report this immediately to ICT.

Users of non-Halton Healthcare devices understand and accept that synchronization relies on one or more cellular network providers and the Internet, and that both are subject to slowdowns and outages of extended duration that are beyond the control of ICT. Halton Healthcare ICT shall support the technology mechanisms within its control to provide reasonable access to Halton-provided services.

Users of non-Halton Healthcare devices agree not to transmit Halton Healthcare sensitive information (e.g., Business Sensitive Information (BSI) or Protected Health Information (PHI)) through non-Halton Healthcare approved methods. Approved methods include those outlined above such as secure transmission via Halton Healthcare email and the One Mail network.

Users of non-Halton Healthcare devices understand that the personal devices can be wiped by Halton Healthcare upon (for purposes outlined above) and understand that this process will delete data including personal files.

Should users have concerns regarding the status of any of the aforementioned protections, or wish further guidance on protecting/encrypting information and/or devices, they may contact the ICT Help Desk (905-845-2571 x7777). Lost or stolen devices must be immediately to the ICT Help Desk 905-845-2571 x7777 who will take the appropriate steps and inform the privacy officer.

1.11 Precautions when Storing and Copying Confidential Information

Confidential Information includes Protected Health Information (PHI) as defined in the Personal Health Information Protection Act (PHIPA), Personal Information (PI) and any financial, statistical, or other information about Halton Healthcare' operations that is not in the public domain. Care must be exercised by all users to ensure electronic copies of confidential information are protected from theft.

1.11.1 Local and Network Folders

Information should not be stored locally on hospital/personal devices (i.e. C:\ drives) and should instead be stored on a network drive (as outlined below). The ICT department maintains a number of network drives where employees are able to store files securely and are backed up regularly:

- P: - Personal (Only the individual user has permissions to this drive/folders)
- S: - Departmental (Only users within the same department have permissions to this drive/folders)
- O: - Common (All Halton Healthcare users have read access to this drive/folders)
- X: - Special (Used in cases where specific intradepartmental staff require access to a shared folder)

1.11.2 Laptop Computers and other Portable Devices

It is particularly important that no PHI and Personal Information is stored on computers or other devices that can be removed from Halton Healthcare premises, as these devices are more vulnerable to theft. Halton Healthcare has a remote access infrastructure that permits users to access all network resources securely from outside the enterprise. In cases where information must be removed from Halton Healthcare network to work off-site or as a result of device ownership, it must be done on an encrypted device or media (please consult the ICT Help Desk 905-845-2571 x7777 to confirm appropriate protections are in-place prior to removal of information). Staff and clinicians who access PHI or BSI routinely from non-Halton Healthcare locations must do so via the approved remote access mechanisms (details for which can be provided by submitting a service request via the ICT Helpdesk.)

1.11.3 Removable Media - Flash Drives/Memory Sticks/CR-RW/DVD-RW

Removable media are considered less vulnerable to theft than mobile devices; however they are more vulnerable to loss and should be treated accordingly. If PHI and Personal Information is copied to removable media, the custodian must exercise due caution to ensure it is protected from unauthorized access. Approval should be obtained as in 1.11.2 if PHI and Personal Information will be removed from Halton Healthcare on removable media, and files stored on these devices must be encrypted.

Key Words

Access to Technology, Privacy and Confidentiality, Intended Use, Acceptable Use, Personal Use, Security, Auditing and Auditing Process, User Codes and Passwords, Internet Use, Social Media, E-mail, Internal E-mail External Mail (Internet mail), Using External Mail to Communicate with Patients, eHealth Ontario ONE Mail, Delegate Access to Halton Healthcare e-mail, Forwarding Mail, Sending Messages to “All Users” and other distribution lists,
Virus Precautions, Out-of-Office Assistant, Disclaimer, Purchase and Installation of Software, Purchase and Installation of IT Equipment/Devices, Personal Equipment and Home Use, Precautions when Storing and Copying Confidential Information, Local and Network Folders, Laptop Computers and other Portable Devices, Removable Media - Flash Drives/Memory Sticks/CR-RW/DVD-RW

Reviewed by/Consultation with

Chief Information Officer
Chief Medical Information Officer
Director, Information and Communication Technology
Manager, ICT Operations and Security

Manager, Network & Telecommunications
Manager, Applications and Integration

Signed by ____

Title ____