1. PURPOSE:

1.1 Use of Information Systems is an essential means for doing business at the Children’s Hospital of Eastern Ontario (CHEO). However, use of the Hospital and services are a privilege, not a right, and therefore must be used with respect and in accordance with the goals of the organization.

1.2 The objectives of this policy are to outline appropriate and inappropriate use of the CHEO information systems and services. This includes general expectations of the User, internet use, electronic mail use, and remote access use which will minimize disruptions to services and activities and ensure systems are used in an efficient, ethical and lawful manner.

2. POLICY:

2.1 Account Activation/Termination

2.1.1 Information systems access at the CHEO is controlled through individual accounts and passwords and is governed by the “Access Control to Information Systems” policy. In addition, to the completed “Information System Access Control” form, each User is required to read the “Information Systems Acceptable Use Policy” and agree to the terms stated under “Acceptable Use of Information Systems Agreement” prior to receiving any system account and password.

2.1.2 Once the Information System Access Control form has been completed and the individual has signed the Acceptable Use of Information Systems Agreement, the individual is deemed to be a “User” of the CHEO’s information systems.

2.1.3 Information systems access will be terminated when the User terminates his/her association with the Hospital. The CHEO is under no obligation to store or forward the contents of an individual systems data after the term of their association has ceased unless other arrangements have been made.

2.2 General Expectations of Users

2.2.1 As CHEO often delivers official communications via electronic mail or by posting to the corporate intranet site (CHEOnet), Users are expected to check their electronic mail and the corporate intranet site in a consistent and timely manner so that they are aware of important announcements and updates, as well as for fulfilling business and role-oriented tasks.
ACCEPTABLE USE OF INFORMATION SYSTEMS

2.2.2 Users are expected to perform effective file and electronic mail message management, including but not limited to:
  • Organization
  • Cleaning and purging
  • Archiving
As well as backup of files and electronic messages stored outside designated locations.

2.2.3 Users are not to attempt to gain access to any data or programs for which they do not have explicit authorization or consent through a signed Access to Information Systems Control Form.

2.2.4 Users are expected to secure their account while logged in by “locking” their active computer session when leaving computer unattended. Users are expected to log out their account at the end of their shift or work day.

2.3 Electronic Mail

2.3.1 Users are expected to remember that electronic mail messages sent from their Hospital account(s) reflects on CHEO’s corporate image and are therefore required to comply with normal standards of professional and personal courtesy and conduct.

2.3.2 Users are to use extreme caution when communicating confidential or sensitive information via electronic mail. Keep in mind that all electronic mail messages sent outside of CHEO become the property of the receiver. A good rule is to not communicate anything that you wouldn’t feel comfortable being made public. Demonstrate particular care when using the “Reply” command during information systems correspondence to ensure the resulting message is not delivered to unintended recipients.

2.3.3 CHEO assumes no liability for direct and/or indirect damages arising from the user’s use of the Hospital’s information systems and services. Users are solely responsible for the content they disseminate. CHEO is not responsible for any third-party claim, demand, or damage arising out of the use of CHEO information systems or services.

2.3.4 All Health Care Providers must follow their College scope of practice or service regarding the use of electronic mail for communicating Personal Health Information. As per the Privacy and Confidentiality policy (Policy No. 10), email of patient health information is strictly prohibited unless a Patient Consent for email Communication (Form 1234) has been obtained from the patient or substitute decision maker.

2.3.5 A standard Hospital disclaimer will be appended to all external bound messages. Users are not to draft and include personal disclaimers in their electronic mail messages.
For all external message, the following disclaimer will be appended to the message:

"This message, including any attachments, may contain confidential information and is for the sole use of the intended recipient(s). Any unauthorized use, disclosure or distribution is prohibited. If you are not the intended recipient, please notify the sender immediately and destroy the original message.

IF THIS MESSAGE INCLUDES MEDICAL INFORMATION, please note that email communication is subject to accidental disclosure or interception by parties not intended to receive the information. Although we have taken precautions to reduce this risk, email communication may not be secure or confidential. If you are receiving medical information by email, you have been advised of the risks and have consented to receiving medical information in this manner. If, at any time, you wish to cease communicating by email, please contact the sender's office or clinic."

2.4 Internet

2.4.1 The Internet is a public forum for business communications and reflects on the Hospital's corporate image and its place in the community. All Users are responsible to maintain and enhance CHEO's public image.

2.5 Remote Access

2.5.1 Users are expected to store sensitive Hospital documents and other printed materials securely in accordance with the Hospitals' "Confidentiality Agreement" (Form No. 6021) while working from a remote location.

2.5.2 Users are expected to disable any automatic log-in tools when connecting to the Hospital's information systems from a remote location.

2.5.3 Users are expected to use a personal firewall on any computer system used to remotely access the Hospital's information systems. Personal firewall settings are enabled by default on all Hospital devices with this functionality. For more information on enabling personal firewall on their personal devices, Users are encouraged to contact either their equipment manufacturer or Internet Service Provider.

2.6 Appropriate Use
ACCEPTABLE USE OF INFORMATION SYSTEMS

2.6.1 Users at CHEO are encouraged to use information systems to further the goals and objectives of the Hospital. The types of activities that are encouraged, but not limited to, include:

- Communicating with fellow CHEO Users, business partners of CHEO, and clients within the context of an individual's assigned responsibilities.
- Acquiring or sharing information necessary or related to the performance of an individual's assigned responsibilities.
- Participating in educational or professional development activities.

2.7 Inappropriate Use

2.7.1 The following activities are deemed inappropriate uses of CHEO Information Systems and services and are prohibited:

- Use of information systems for illegal or unlawful purposes, including copyright infringement, obscenity, libel, slander, fraud, defamation, plagiarism, harassment, intimidation, forgery, impersonation, soliciting for illegal pyramid schemes, and computer tampering (e.g. spreading of computer viruses or other malicious software).
- Use of information systems in any way that violates the Hospital's policies, rules, or administrative orders.
- Creating, viewing, copying, altering, or deletion of information systems accounts or data belonging to the Hospital or another individual without authorized permission.
- Sending of unreasonably large information systems attachments. The total size of an individual information systems message sent in one message (including attachment) should be 10,000 KB or less.
- Opening email attachments from unknown or unsigned sources such as email attachments are the primary source of computer viruses and should be treated with utmost caution.
- Sharing information system account passwords with another person, or attempting to obtain another person's information system account password. Information system accounts are only to be used by the registered user.
- Excessive personal use of the Hospital's information system resources. CHEO allows limited personal use for communication with family and friends, independent learning, and public service so long as it does not interfere with staff productivity, pre-empt any business activity, or consume more than a trivial amount of resources. CHEO prohibits personal use of its information systems and services for unsolicited mass mailings, non-Hospital commercial activity, political campaigning, dissemination of chain letters, and use by non-users. The Hospital reserves the right to restrict access to internet sites it considers inappropriate for the workplace.

2.8 Monitoring and Confidentiality
2.8.1 The information systems and services used at CHEO are owned, leased, or in the custody of the organization and are therefore its property. This gives CHEO the right to monitor any and all information traffic passing through its systems. This monitoring may include, but is not limited to, inadvertent reading by Information Services staff during the normal course of managing the information system, review by the legal team during the information system discovery phase of litigation, observation by management in cases of suspected abuse or to monitor user efficiency.

2.9 In addition, archival and backup copies of information systems data may exist, despite User deletion, in compliance with CHEO records retention practices. The goals of these backup and archiving procedures are to ensure system reliability, prevent data loss, meet regulatory and litigation needs, and to retain corporate knowledge.

2.10 Backup copies exist primarily to restore service in case of failure. Archival copies are designed for quick and accurate access by CHEO delegates for a variety of management and legal needs. Patient Health Information backups and archives retention is governed by the Children’s Hospital of Eastern Ontario’s “Retention and Destruction of Patient Health Records” policy (Policy No. 69) while Business Records retention is governed by the Income Tax Act. The retention period is as follows:
   - Patient Records: Patient Information must be kept for a minimum of 10 years past the patient’s eighteenth birthday.
   - Business Records: Business records must be kept for a minimum of six years from the end of the latest year to which they relate.

2.11 If CHEO discovers or has sufficient reason to suspect activities that do not comply with applicable laws or this policy, information systems records may be retrieved and used to document the activity in accordance with due process. All reasonable efforts will be made to notify the User if his or her information system records are to be reviewed. Notification may not be possible, however, if the User cannot be contacted or if notification will defeat the purpose of an ongoing investigation.

2.12 Hospital users are strongly discouraged from saving any identifiable patient information outside of Hospital Information Systems to portable IT equipment and removable media. Users must take appropriate steps to protect privacy and confidentiality of the patient if information leaves the Hospital premises on portable IT equipment, removable media or as electronic mail or file transfer. Possible safeguards that can be used include but not limited to:
   a. Password-protected files. The password should be communicated over the phone or in separate email
   b. Encrypted media
   c. Communicate de-identified information
   d. Use approved secure communication (VPN Access)
ACCEPTABLE USE OF INFORMATION SYSTEMS

2.13  Failure to Comply

2.13.1  Violations of this policy will be treated like other allegations of wrongdoing at the CHEO. Allegations of misconduct will be adjudicated according to established procedures. Sanctions for inappropriate use on the CHEO’s information systems and services may include, but are not limited to, one or more of the following:
• Temporary or permanent revocation of information systems access;
• Disciplinary action according to applicable CHEO policies;
• Termination of employment; and/or legal action according to applicable laws and contractual agreements.

3. SCOPE:

3.1  All Information Systems and services owned, leased, or in the custody of the CHEO.

3.2  All Information Systems account users/holders at the CHEO.

3.3  All CHEO Information Systems records.

4. DEFINITIONS:

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archiving</td>
<td>Act of storing files for historical interest.</td>
</tr>
<tr>
<td>Designated locations</td>
<td>Designated locations are network file shares (example: J:\ Drive).</td>
</tr>
<tr>
<td>Electronic Mail</td>
<td>Electronic mail, often abbreviated to e-mail, is any method of creating, transmitting, or storing primarily text-based human communications with digital communications systems.</td>
</tr>
<tr>
<td>Firewall</td>
<td>Is a dedicated appliance or software running on another computer, which inspects network traffic passing through it, and denies or permits passage based on a set of rules.</td>
</tr>
<tr>
<td>Individual</td>
<td>Any person who does not meet the criteria of “User”.</td>
</tr>
<tr>
<td>Information Systems</td>
<td>Any computerized data processing or storage system.</td>
</tr>
<tr>
<td>Internet</td>
<td>The Internet is a global system of interconnected computer networks that interchange data by packet switching using the standardized Internet Protocol Suite (TCP/IP). It is a &quot;network of networks&quot; that consists of millions of private and public, academic, business, and government networks of local to global scope that are linked by copper wires, fiber-optic cables, wireless connections, and other technologies.</td>
</tr>
</tbody>
</table>

Approved by: Executive Team  Date: April 20, 2010
Revision Number: 1
## ACCEPTABLE USE OF INFORMATION SYSTEMS

<table>
<thead>
<tr>
<th><strong>IT Equipment</strong></th>
<th>Is any computing hardware used to access, process and store or transmit Hospital information (ex. PC or server). Portable IT equipment includes laptop, tablet PC, handhelds and smartphones.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Personal Firewall</strong></td>
<td>A personal firewall is an application which controls network traffic to and from a computer, permitting or denying communications based on a security policy. A personal firewall differs from a conventional firewall in terms of scale. Personal firewalls are typically designed for use by end-users. As a result, a personal firewall will usually protect only the computer on which it is installed.</td>
</tr>
<tr>
<td><strong>Personal Health Information</strong></td>
<td>Personal Health Information: Personal Health Information is identifying information about an individual that, (a) relates to the physical or mental health of the individual, including health history of the individual's family, (b) relates to the providing of health care to the individual, including the identification of the care provider (c) relates to payments or eligibility for health care in respect of the individual, (d) relates to the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance, (e) is the individual's health number, or (f) identifies an individual's substitute decision-maker.</td>
</tr>
<tr>
<td><strong>Remote Access</strong></td>
<td>Is the ability to access a CHEO computer, network drive, or application from a remote location. Remote access is applicable to many forms of connectivity methodologies including but not limited to dial-up, VPN, and Citrix.</td>
</tr>
<tr>
<td><strong>User</strong></td>
<td>An individual who has authorized access to the Children’s Hospital of Eastern Ontario’s information systems and has signed the Acceptable Use of Information Systems Agreement.</td>
</tr>
<tr>
<td><strong>VPN Access</strong></td>
<td>Is a connectivity method that creates a secure tunnel connection between remote user/location and company IT resources over a public network infrastructure such as Internet. Data passing between the two ends of the tunnel is encrypted.</td>
</tr>
</tbody>
</table>

### 5. RESPONSIBILITY:

5.1 Users are responsible:
ACCEPTABLE USE OF INFORMATION SYSTEMS

5.1.1 • of ensuring conditions set out in this policy are adhered to
  • to check their electronic mail and the corporate intranet site in a
    consistent and timely manner
  • for effective file and email management
  • to protect the confidentiality of his or her account and password
    information. Sharing of passwords is strictly prohibited as activity
    that occurs under the account is the responsibility of the person
    holding that account password
  • for changing their passwords at least once every six (6) months.
These rules are in place to protect the User and the CHEO. The
passwords must be at least (8) eight characters long. They must
include at minimum both upper and lower case characters as well
as both alpha and numeric characters with the exception of Mobile
Telecommunication Devices where the password, at a minimum
must be four (4) characters in length. Where possible, these
requirements will be enforced by system security administration
settings.
  • for the accuracy and appropriateness of data they enter into the
    CHEO’s information systems.
  • for treating all electronically stored patient and hospital data as
    confidential and will only disclosing information to individuals who
    are authorized to receive such information.

5.1.2 "Remember Password" feature are not be used with any
application.

5.1.3 Use of the same password for the CHEO accounts as for other
non-Hospital access (e.g. personal bank account) is discouraged.

5.1.4 In the event the User has reason to believe that his/her access
codes have been compromised, the User must immediately contact
the Service Desk to make arrangements for new passwords.

5.2 Health Care Providers are responsible:

5.2.1 • for following their College or other professional scope of practice
  or service regarding use of electronic mail for communicating
  Personal Health Information.

5.3 Information Services are responsible:

5.3.1 • to ensure system account and passwords are only given to
  Users who have agreed to the terms in this policy by signing the
  “Acceptable Use of Information Systems Agreement Form”.
  • to ensure proper system backups and electronic archives are
    taken and stored in coordination with the policies governing patient
    and business record retention.
  • to ensure all external-bound electronic messages have the
    corporate disclaimer appended to the message.

6. PROCEDURE:

6.1 Reporting Misuse

Approved by: Executive Team                        Date:  April 20, 2010
Revision Number: 1
ACCEPTABLE USE OF INFORMATION SYSTEMS

6.1.1 Any allegations of misuse should be promptly reported to the individual's immediate supervisor. If you receive an offensive email, do not forward, delete, or reply to the message. Instead, report it directly to the individual named above.

7. CROSS-REFERENCES: 7.1 Retention And Destruction Of Patient Health Records Policy
                          7.2 Access Control to Information Systems Policy
                          7.3 Confidentiality Agreement (Form No. 6021)

8. REFERENCES: 8.1 Income Tax, Information Circular (Ic05-1) Electronic Record Keeping, June 2005

9. ATTACHMENTS: 9.1 Brian Vezina, Senior Business Systems Analyst, Information Services
                    9.2 Pavlo Ignatusha, Manager, Information Services
                    9.3 Louise Martin, eHealth Coordinator