KINGSTON HEALTH SCIENCES CENTRE

ADMINISTRATIVE POLICY MANUAL

Subject: Auditing of Access to Hospital Electronic Data and Information **Number: 01-155**

Page:	1 of 3
Original Issue:	2017.04
Revised:	NEW

Issued by: President and Chief Executive Officer

Principle:

Federal and Provincial legislation requires hospitals to take steps that are reasonable in the circumstances to ensure information in their custody or control is protected against theft, loss, unauthorized access, use or disclosure.

The Privacy Office will conduct and monitor access to Personal Health Information (PHI) and other confidential information contained within the information systems of Kingston Health Sciences Centre (KHSC), eHealth Ontario, and other regional/provincial systems, to ensure compliance with organizational and legislative requirements.

Definitions:

Agent: A person who acts on behalf of the custodian in exercising powers or performing duties with respect to personal/private information whether or not employed (or remunerated) including volunteers, students, physicians, consultants, nurses, vendors and contractors.

Audit: A manual or systematic assessment of end user access to an information system that may include: Complaint/Concern Based Audit, Media Attracting Person (MAP) Audit, Proactive Audit, Random Audit, or Trigger Audit.

Circle of Care: The "circle of care" is not a defined term under PHIPA. It is a term of reference used to describe the provisions of PHIPA that enable custodians to rely on an individual's assumed implied consent when collecting, using or disclosing personal Health information for the purpose of providing or assisting in providing health care.

Information Systems: For the purposes of this policy, refers to any system containing confidential hospital information.

User: An agent of the hospital who has a user account and is identified in the system by a user ID and password.

Policy:

1. KHSC has a legal and ethical responsibility to ensure that all information in its custody and control is protected against theft, loss, unauthorized access, use or disclosure in any format, including information that is contained in the information systems.
2. New staff and agents are required to complete privacy and confidentiality education and sign a confidentiality agreement as a condition of employment or affiliation. Regular communication on privacy issues is circulated to all staff and agents. Contracted agents are bound to privacy and confidentiality as a condition of their contract.
3. Accessing any patient information in all of the information systems to which KHSC has access is only permitted by the circle of care for the purpose of providing health care to the patient and/or in the performance of your duties as an agent of the hospital on a "need to know basis."
4. Users will be held accountable for any and all activity carried out in the information systems under his/her password.
5. All access to information in the systems is logged by default, monitored and audited regularly to ensure compliance with organizational and legislative requirements. Where an audit by the Privacy Office reveals irregularities to a KHSC information system, investigations will be conducted in collaboration with the department Supervisor/Manager or delegate. Where an audit by the Privacy office reveals irregularities to eHealth Ontario and/or other

regional/provincial systems, KHSC will report these to eHealth Ontario and/or other regional/provincial systems as appropriate.

6. Any unauthorized access, use or disclosure may result in suspension or termination of your access privileges and disciplinary action up to and including termination of employment or affiliation or sanctions as specified in law.

Procedure:

1. KHSC Privacy Office/delegate will conduct electronic access audits within the information systems. Examples of audits are:
    a. **Complaint/Concern Based Audit:**
    An audit conducted as a result of the Privacy Office receiving a concern or complaint.
    b. **Media Attracting Person (MAP) Audit:**
    A clinical system audit conducted on a patient who has garnered public interest.
    c. **Proactive Audit:**
    An audit based on specific high risk user activity. Examples include: similar last name, large number or accesses, etc.
    d. **Random Audit:**
    A scheduled audit conducted where patients or users are selected randomly. Consent directives (lock-box requests) are also audited on a scheduled basis to ensure accuracy and appropriateness.
    e. **Triggered Audit:**
    A more detailed audit conducted in response to a correlated Complaint/Concern Based, MAP, Proactive or Random Audit.
2. The Privacy Office will review audits for user compliance and/or circle of care inclusion.
3. If the access is established to be unauthorized and outside of the authorized role of the user, the appropriate action to be taken may include any or all of the following:
    a. Education/privacy training;
    b. Re-signing of the agent's confidentiality agreement;
    c. Follow up audits;
    d. Suspension;
    e. Notification to the agent's Regulatory College;
    f. Disciplinary action up to and including termination of employment or affiliation;
    g. Notification to Information and Privacy Commissioner of Ontario.
4. The Privacy Office will maintain a case file and log of all audits generated.
5. Case files will be securely retained and destroyed in accordance with the KHSC records retention schedule.

Related Policies:
01-210 Electronic Security Authorization and Authentication
01-217 Business Conduct
01-220 Records Management
01-221 Privacy Practices
01-225 Privacy Breach Management
09-050 Disclosure of Personal Health Information
09-055 Personal Health Information Protection
09-140 Access to and Correction of Personal Health Information
12-320 Code of Behaviour

Authorizing Signature:

Dr. David Pichora
President and Chief Executive Officer