KINGSTON HEALTH SCIENCES CENTRE

ADMINISTRATIVE POLICY MANUAL

Subject:	**Privacy Practices**	**Number:**	**01-221**
		Page:	1 of 5
Issued by:	President and Chief Executive Officer	Original Issue:	2017.04
		Revised:	2018.11

Introduction:
Kingston Health Sciences Centre (KHSC) is committed to protecting the confidentiality of all information in its custody and control, whether it is written, verbal, electronic, or other form. All persons employed, appointed, and affiliated with KHSC who collect, use or disclose this information on KHSC's behalf are required to follow the ten information principles below. Confidential information of the hospital includes personal information (e.g. employee file); personal health information (e.g. patient care information); and business information (e.g. contracts or agreements).

Policy Statement:
KHSC respects privacy as a fundamental human right that is central to the dignity of the individual. We recognize that personal health information (PHI) belongs to the individual to whom it relates and that we are simply its custodian as required by law.

Our practices are guided by the ethical principles of professional codes of practice, Hospital By-Laws and the federal and provincial laws that govern the collection, use and disclosure of information, like the Personal Health Information Protection Act, 2004 (PHIPA), the Freedom of Information and Protection of Privacy Act, 2012 (FIPPA), and The Public Hospitals Acts, 1990, to name a few.

Definitions:
Affiliate: an individual who is not employed by the hospital but performs specific tasks at the hospital, including: learners, volunteers, contractors or employees of contractors who may be members of a third-party contract or under direct contract to the hospital, and individuals working on the hospital premises, but funded/employed through an external source (i.e. research and university staff on site).

Breach: The unauthorized collection, use, disclosure, retention, or disposal of confidential information in a manner that contravenes privacy legislation. Breaches can be accidental or intentional. This includes unauthorized access/and viewing by an individual who is not involved in providing or assisting with the care of a patient.

Confidential Information: Confidential information includes information, in any format, created or received by the hospital in the course of its business, including patient information, Executive and Corporate information (including, but not limited to, information pertaining to the hospital medical staff, Board and Executive Committee meeting minutes, working drafts of corporate documents), financial information, human resources information (including, but not limited to, payroll, personnel, or legal information, and staff health records), that is not intended for members of the public.

Health Information Custodian (HIC): As defined in the PHIPA, 2004 states a "person or organization who has custody or control of Personal Health Information as a result of or in connection with performing the person's or organization's powers or duties or the work as described in section 3 (1) of the act."

Health Information Network Provider (HINP): is defined as a person (which includes organizations) who provides services to two or more health information custodians (HICs)

where the services are provided primarily to HICs to enable the HICs to use electronic means to disclose PHI to one another, whether or not the person is an agent of any of the custodians.

Privacy Impact Assessment (PIA): is a formal risk management tool used to identify the actual or potential effects that a proposed or existing information system, technology or program may have on individuals' privacy. A PIA also identifies ways in which privacy risks can be mitigated.

Workplace: All hospital premises, work assignments that occur off hospital property, off site work-related social events and functions, work-related seminars, conferences, travel and training, and other locations where work related responsibilities are carried out. Phone calls, communications, faxes, and electronic mail that are related to workplace activity made with communication devices are considered an extension of the workplace

Policy:

1. *Accountability for Confidential Information*
   KHSC is responsible for all confidential information under its custody and control and has designated an individual as Privacy Officer who is accountable for ensuring the organization's compliance with these principles. KHSC will:
   a) Implement policies and procedures to protect all confidential information.
   b) Respond to complaints and inquiries.
   c) Educate all persons employed, appointed, and affiliated at KHSC about privacy policies and practices as well as their duties when they relate to privacy and confidentiality of information. As a condition of employment, all new KHSC employees/agents must sign a confidentiality agreement. The KHSC Privacy Office conducts continuous privacy awareness education to foster and promote a culture of privacy. Education will be delivered to ensure employees, agents and third parties are provided with tools, training and support as appropriate to enable them to fulfill their duties as they relate to the privacy of all confidential information.
2. *Identifying Purposes for the Collection of Confidential Information*
   KHSC will identify the purposes for which confidential information is collected at or before the time of collection. These will be conveyed electronically or by means of posters and brochures or on forms used to collect the information. PHI is used to deliver direct patient care; for administration and management of the health care system locally, regionally, and provincially; for research, teaching and statistics; for fundraising and to meet legal and regulatory requirements.
3. *Consent*
   KHSC will collect, use and disclose confidential information with the knowledge and consent of the patient except where permitted by law. A patient may withdraw consent for use and disclosure of his/her PHI at any time, subject to legal or contractual restrictions and reasonable notice. KHSC will inform the individual of the implication of such withdrawal. KHSC may use or disclose PHI for purposes, including research, without an individual's consent if strict conditions are met.
4. *Limiting Collection of Confidential Information*

KHSC will limit the collection of confidential information to that which is necessary for the purposes identified. Information will be collected by fair and lawful means.

5. *Limiting Use, Disclosure, and Retention of Confidential Information*
   KHSC will not use or disclose confidential information for purposes other than those for which it was collected, except with the consent of the individual or as required by law, collective agreement or other policies. Confidential information will be retained only as long as necessary for the fulfilment of those purposes, and as required by law. KHSC has established information retention guidelines that define consistent minimum standards and requirements for the length of time PHI, personal and business information is to be maintained. Confidential information will be securely destroyed in accordance with legislation, hospital policies, guidelines and procedures. KHSC has also established appropriate practices for the timely and secure disposal of PHI consistent with confidentiality, legal and regulatory requirements.
   Researchers are responsible for the storage, retention and destruction of research data at minimum for the length of their appointment at KHSC or as required by regulatory bodies, whichever is greater.
6. *Accuracy of Confidential Information*
   KHSC will make every effort to ensure the information held is accurate, complete and up-to-date.
   A patient will be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
7. *Safeguards for Confidential Information*
   KHSC applies security safeguards appropriate to the sensitivity of confidential information to protect it against loss, theft, unauthorized access, disclosure, copying, use, or modification, regardless of its format. Protection may include physical measures (e.g. locked filing cabinets and restricted access), organizational measures (e.g. limiting access on a "need-to-know" basis), and technological measures (e.g. use of passwords, encryption and audits). If necessary to transport documentation containing confidential information outside of the hospital, it should be secured in a closed container (e.g. briefcase, bankers box, chart carrier, zippered bag). Chart containers should be lockable if possible or, if transported in a private vehicle, confidential information should be transported in a locked trunk. Confidential information should never be left unattended.
   New staff and affiliates 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 affiliates. Contracted agents are bound to privacy and confidentiality as a condition of the contract. All breaches of confidential information will be brought to the immediate attention of the KHSC Privacy Officer. The KHSC Privacy Office will adhere to the Privacy Breach Management processes and procedures outlined in the 2006 Ontario Information and Privacy Commissioner (IPC) protocol “What to Do When Faced with a Privacy Breach”.
   As a health information custodian, as a participant of eHealth Ontario and regional/provincial health information systems, and as a health information network provider (HINP) KHSC

conducts privacy impact assessments (PIA) and threat risk assessments (TRA) as required and recommended by PHIPA and the Information Privacy Commissioner of Ontario (IPCO).

8. *Openness About Confidential Information Policies and Practices*
   KHSC will make information about its privacy policies and practices available by means of posted notices and brochures at registration points and other public areas as well as on the hospital's Internet site. Information provided includes:
   a) Contact information for the KHSC Privacy Office, to which complaints or inquiries can be forwarded.
   b) The process for a patient to access his/her PHI held by the hospital.
   c) A description of the type of PHI held by the hospital, including a general explanation of its use, and common examples of how the information may be shared.
9. *Individual Access to Own Confidential Information*
   Upon request, KHSC will inform an individual of the existence of their confidential information and will be given access to that information as allowable under applicable legislation, collective agreements or policy. For PHI contact Release of Information at (613) 544-3400 Ext. 4125. For employee access to their own personnel file contact Human Resources-HDH site at (613) 544-3400 Ext. 2381; People Services and Organizational Effectiveness-KGH site at (613) 549-6666 Ext. 2365. For personal information (non-health) contact the Freedom of Information/Privacy Office at (613) 549-6666 Ext. 2567. Fees may apply for accessing or receiving copies of information.
   An individual may request correction of their confidential information as allowable by law and indicated in procedures. This does not include changing the medical opinion of an author recorded in a patient record.
10. *Challenging Compliance with Hospital Privacy Practice*
    An individual will be able to address a concern with compliance of this policy to the KHSC Privacy Officer. It is encouraged that concerns be dealt with through the local Privacy Officer, however if resolution is unsatisfactory, a complaint may be made to the Information & Privacy Commissioner/Ontario. The Commissioner is located at 2 Bloor St. E, Suite 1400, Toronto, ON, M4W 1A8; telephone (416) 326-3333 or 1-800-387-0073.

    The KHSC Privacy Office will monitor adherence to this policy using a risk-based model, and report to the appropriate governing bodies. Accountability for KHSC compliance with this policy rests with the President and Chief Executive Officer or delegate, although other individuals within KHSC, authorized agents, and/or third parties will be responsible for the day-to-day collection and processing of PHI. Breach of this policy and related privacy policies may be subject to disciplinary action as outlined in KHSC policy.

References:

- Privacy by Design, Office of the Privacy Commissioner Ontario, January 2009
- A Policy is Not Enough: It Must is Reflected in Concrete Practices, Office of the Privacy Commissioner Ontario, September 2012
- 10 Privacy Principles, Canadian Standards Association

- 2011 Guidelines for the Protection of Health Information, COACH: Canada's Health Informatics Association
- What to Do When Faced with a Privacy Breach. Information and Privacy Commissioner of Ontario, 2006

Related Policies:
01-132 Mobile Phone Usage
01-139 Security of and Access to Hospital Electronic Data & Information
01-146 Email Usage
01-151 Social Media
01-155 Auditing of Access to Hospital Electronic Data and Information
01-165 Health Information Network Provider
01-210 Electronic Security Authorization and Authentication
01-217 Business Conduct
01-219 Freedom of Information
01-220 Records Management
01-222 Use of Cell Phone Cameras and Recording Devices
01-225 Privacy Breach Management
02-075 Use of Wireless Communication Devices in Proximity to Medical Equipment
06-120 Medical Photography: Photographs/Audio Visual Recording
06-170 Incident Reporting
09-050 Disclosure of Personal Health Information
09-054 Consent Management/Lock-box
09-055 Personal Health Information Protection
09-130 Patient Information for Research/Teaching/Utilization
09-140 Access to, Correction and Use of Personal Health Information
09-150 Duplication of Personal Health Information
09-160 Release of Original Patient Record Out of Hospital
09-180 Patient Records: Medical Records Retention/Destruction
11-150 Health Research

Authorizing Signature

_____

Dr. David Pichora
President and Chief Executive Officer