KINGSTON HEALTH SCIENCES CENTRE

ADMINISTRATIVE POLICY MANUAL

Subject: Privacy Breach Management **Number: 01-225**

Revised: 2017.04

Preamble:
Under the Personal Health Information Protection Act (PHIPA) 2004 and the Freedom of Information and Protection of Privacy Act (FIPPA) 2012, Kingston Health Sciences Centre (KHSC) protects confidential information relating to patients, employees and the business of the organization. All agents are responsible for ensuring that information to which they have access is kept confidential and private.

All KHSC agents have a responsibility to report privacy breaches as required by legislation.

Policy Statement:
This policy applies to KHSC confidential information contained within the hospital's information systems and eHealth Ontario and other regional/provincial systems to which KHSC has access.

Definitions:
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.

Examples include:

- A patient is discharged home with another patient's medical information.
- A confidential fax is inadvertently sent to an external recipient not authorized to receive the information.
- Lost confidential information or device (e.g. USB key) that is found by a member of the public.

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.

Incident: An event that contravenes hospital and/or departmental policy/procedure and if not intercepted, has the potential for breach.

Examples include:

- Lost or misplaced confidential information or device (e.g. USB key) belonging to an agent that is recovered by an agent.
- Compromised passwords
- Hacker attacks

Personal Health Information: Personal health information means "identifying information" about an individual in oral or recorded form, if the information:

a) Relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family;
b) Relates to the providing of health care to the individual, including the identification of a person as a provider of health care to the individual;

c) Is a plan of service within the meaning of the Long-Term Care Act, 1994 for the individual;
d) Relates to payments or eligibility for health care in respect of the individual;
e) 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;
f) Is the individual's health number; or
g) Identifies an individual's substitute decision-maker.

Personal Information: Information about an individual that identifies the individual or that can be linked or matched by a reasonably foreseeable method to other information that identifies the individual. Personal information can be information about a physician or other care provider, a hospital staff person, a patient, or patient's family member.

Policy:

1. All KHSC agents must immediately report privacy incidents/breaches to the KHSC Privacy Office and/or log the occurrence in SAFE Reporting (including all pertinent details).
2. The KHSC Privacy Office will be alerted to all confidential information breaches and will adhere to their in-house Protocol for breach management.
3. Patients will be notified if their information is breached. When required, the Privacy Office will also notify eHealth Ontario and other regional/provincial program offices, as appropriate.
4. Information security incidents/breaches may be logged by both Customer Support Services and the Privacy Office who will follow internal protocols for managing the incident/breach and preventing further occurrences.