Privacy, Confidentiality and Security of Information Policy		
Date first created: January 2004	**Revised:** August 2016	**Approved By:** Chief Privacy Officer

PREAMBLE

Baycrest respects the right of each individual to privacy, and to the confidentiality of their Personal Information and Personal Health Information. In addition to its obligation to respect the privacy of the individual, Baycrest recognizes that certain information pertaining to the Baycrest organization, such as financial and human resource information, is and should remain confidential.

Baycrest staff and volunteers are bound by the Baycrest Code of Conduct to protect the privacy and confidentiality of information.

Definitions

"Baycrest staff" means Baycrest employees, appointed medical staff, clinical and research fellows, scientists, students, and volunteers who are given access to Confidential Information.

"Confidential Information" means Personal Information, Personal Health Information and Confidential Baycrest Business Information:

"Confidential Baycrest Business Information" means information relating to Baycrest as an organization that is not otherwise available to the public such as:

i. Business information including strategic initiatives, organizational restructuring, outsourcing business, negotiations;
ii. Personnel Information on employees, students, volunteers, such as Personal Information maintained by the Human Resources Department, Occupational Health & Safety Department.
iii. Legal information including legal advice, contracts, litigation, and potential claims;
iv. Information relating to research, intellectual property (Policy on Intellectual Property), and quality management; and
v. Information related to fundraising.

"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 *Home Care and Community Services Act, 1994* for the individual,

(d) relates to payments or eligibility for health care, or eligibility for coverage 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" means recorded information about an identifiable individual, including,

(a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,

(b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

(c) any identifying number, symbol or other particular assigned to the individual,

(d) the address, telephone number, fingerprints or blood type of the individual,

(e) the personal opinions or views of the individual except where they relate to another individual,

(f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,

(g) the views or opinions of another individual about the individual, and

(h) the individual's name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual;

POLICY

Baycrest staff are responsible for maintaining the confidentiality of Confidential Information whether it is conveyed verbally, in writing, electronically, in photograph, on film or by other means.

Removal of Confidential Information from Baycrest premises is prohibited except in transit between Baycrest locations and/or when necessary for the provision of health care. When in transit, Confidential Information must be securely stored and in the custody and control of the individual at all times.

Baycrest staff may disclose information already made public by Baycrest elsewhere in publications or on Baycrest's web site, for example. However, information on the Baycrest Intranet may be Confidential Information.

If a staff person is unsure whether information relating to Baycrest is confidential and should not be disclosed, the staff person should check with his or her supervisor.

Personal Information

In the course of their duties at Baycrest, a Baycrest staff person may collect, use and disclose (i) Personal Information about an individual in accordance with Freedom of Information, and (ii) Personal Health Information in accordance with Personal Health Information.

A staff person's authority to access information is limited and strictly confined to information required for performance of the Baycrest staff person's current Baycrest duties.

Employee Personal Information

Access to an employee's record in Human Resources must be done in accordance with the Human Resources Employee Records Policy, Employee Health Records Accessibility and the Occupational Health and Safety Policy, Confidentiality of Health Information.

Communicating Verbally

Confidential Information should not be discussed in a location when others not entitled to receive that information are present, such as:

- In public areas of Baycrest including elevators, washrooms, hallways, stairwells and the cafeteria;
- At home;
- In public places outside Baycrest.

Communicating Confidential Information Externally through Electronic Means (Fax, USB memory keys, E-Mail, text messaging, Internet, or any other electronic methods)

Electronic data must be protected. Personal health information and other Confidential Information may not be stored on mobile computing devices. All Confidential Information must only be stored on Baycrest servers. Access to Confidential Information is available via remote access software provided by Baycrest. In addition to restricting storage to Baycrest servers, all Baycrest laptops must be encrypted. Exceptions to these situations are considered on an individual basis and only with the expressed authority of the Chief Privacy Officer and when transfer or storage of confidential or personal health information is on a temporary basis, using encrypted media and processes to permanently delete the data from the temporary storage media after the transfer has occurred.

External transmission of Confidential Information must be sent securely to protect privacy (Appropriate Use of the Internet, E-mail, Electronic Devices Policy and Fax Transmission of Confidential Client Information). E-Health will provide the tools and software to enable encryption of laptop devices as they

are deployed. Baycrest staff using their own electronic devices for the purpose of Baycrest work are subject to these restrictions around Confidential Information.

Computer Security

Computer access is controlled by passwords at Baycrest. Baycrest staff must not disclose their passwords to any individual whether that individual is another Baycrest staff person or an outside person.

Baycrest staff members must choose a password to use that is not easy to guess. The user's name, the name of the user's relative, and the name of a pet are not acceptable passwords. Baycrest requires the use of an 8 character password that has a combination of upper and lower case letters and must include one numeric character.

Baycrest staff must never post their passwords on workstations or any location where the password may be discovered.

If a password has been observed, guessed or inadvertently shared, the Baycrest staff member must change it immediately.

When finished with using the computer or if interrupted, a Baycrest staff member should sign off, ensure the computer returns to a password menu before leaving their workstation or use a screen-saver password.

All workstations (including, but not limited to desktops, laptops, tablet PCs, thin clients, and personal digital assistants/smartphones that access Baycrest business and clinical systems are subject to the requirements outlined in this policy.

- All Confidential Information must be stored only on the appropriate Baycrest networked servers, to prevent data loss, data compromise, privacy breach, and to ensure backup of the data. No Confidential Information may be stored on local drives or mobile devices.
- Mobile devices (notebooks, tablets, etc.) managed by Baycrest E-Health are subject to the Mobile Computing Policy and must be encrypted using standard full-disk encryption software as defined by the Manager of Technical Services & Customer Support. Other workstations and devices may be encrypted as deemed necessary by the Chief Privacy Officer.

Information available on computer screens should be protected in order to limit viewing by unauthorized persons.

Fundraising

Information about clients to be disclosed to the Baycrest Foundation for the purpose of fundraising will be disclosed with consent or as permitted by law. Individuals will have an opportunity to decline to have their information used for fundraising purposes (see Release of Personal Information to the Baycrest Foundation).

PROCEDURES

1. Baycrest and departmental Managers will make available written materials about Baycrest's privacy policies and information practices. Baycrest staff are encouraged to familiarize themselves with Baycrest's Privacy Code, which is available on Baycrest's Intranet.
2. Managers with Baycrest staff will review the Privacy, Confidentiality and Security of Information Policy and Procedures. This policy will be available on Baycrest's Intranet.
3. New Baycrest staff will be provided detailed information about their accountability for ensuring the confidentiality of Personal Information and Personal Health Information, during the Baycrest New Staff Orientation. Baycrest volunteers will be oriented to the Privacy Confidentiality and Security of Information Policy during the formal Volunteer Orientation. New physicians and medical students will be oriented to the Privacy, Confidentiality and Security of Information Policy by their clinical supervisor when they begin working at Baycrest.
4. Each person approved for access to Baycrest information systems will, after being oriented to the Confidentiality and Security of Information Policy, be given a personal Login Identification or Password by Customer Service and Support.
5. No one with authorized access to Baycrest electronic information systems will share their Login Identification Password.
6. If Confidential Information is lost, stolen or subject to unauthorized access, use or disclosure, the individual who is responsible for it on Baycrest's behalf must report the incident in writing, providing a brief description of the information, the date and time of the incident, their name and department, to the Chief Privacy Officer. The incident must also be reported in the Safety Event Reporting System (SERS).
7. Periodic audits of confidential electronic records will be conducted by the Chief Privacy Officer to monitor and assess compliance with Baycrest policies. Any potential concerns arising from the audits will be reviewed with the user's manager and, and other managers and may also include the Executive Director of Human Resources.
8. If it is established that a breach of privacy has occurred, those individuals deemed responsible may be subject to penalty or sanction up to and including termination of employment, cancellation of contract or services, termination of the relationship with Baycrest, or withdrawal of privileges. Legislation protects a person who prevents a breach of privacy or reports a breach or a plan to breach privacy to Baycrest management or to a government privacy commissioner. A person who does so, if acting in good faith and on reasonable belief, may not be dismissed, suspended, demoted, disciplined, harassed or otherwise disadvantaged.
9. The Privacy, Confidentiality and Security of Information Policy and related procedures will be reviewed annually as part of the Core Curriculum, along with Baycrest's Privacy Code.

CROSS-REFERENCED POLICIES:

1. Appropriate Use of Internet, E-mail, Electronic Devices
2. Confidentiality of Health Information
3. Employee Health Records – Accessibility
4. Fax Transmission of Confidential Client Information
5. Freedom of Information
6. Intellectual property
7. Personal Health Information

APPENDIX:

Confidentiality & Security Agreement Form
Privacy Breach Protocol

CONFIDENTIALITY and SECURITY AGREEMENT

1. I have read and understood Baycrest's Privacy, Confidentiality and Security of Information Policy; Baycrest's Appropriate Use of Internet, E-mail and Electronic Devices Policy; and the Baycrest Privacy Code (the "Policies"). I agree to abide by the terms of the Policies.

2. I agree to keep confidential any information obtained during the course of my relationship with Baycrest. "Confidential Information" includes, but is not limited to, any oral, written or electronic personal health information, personal information or business information relating to the management of Baycrest, including information about its patients, residents, clients, staff, students and volunteers.

3. I understand that all personal health information to which I have access through my relationship with Baycrest is Confidential Information and under the *Personal Health Information Protection Act, 2004*, I have the legal obligation to protect individual privacy and the confidentiality of personal health information.

4. I will only collect, use and disclose Confidential Information strictly for the performance of my duties at Baycrest. I will not collect, use or disclose more Confidential Information than is reasonably required for my role.

5. I am familiar with Baycrest's Policies that govern the handling of Confidential Information, including the following requirements:

- I agree to keep my passwords (including user names) to Baycrest's electronic information systems confidential and secure. I understand that I am accountable for all actions performed when an electronic information system has been opened using my access code.
- I understand that Confidential Information must only be stored on Baycrest servers. If I am authorized to transfer Confidential Information via a mobile computing device (such as a USB key or laptop), the device must be encrypted.
- Removal of Confidential Information from Baycrest's premises is prohibited except in transit between Baycrest locations or when necessary for the provision of health care. When in transit, Confidential Information must be securely stored.

6. I shall immediately report all incidents involving loss, theft or unauthorized use or disclosure of Confidential Information to my immediate supervisor/manager and to Baycrest's Chief Privacy Officer.

7. I understand and acknowledge that Baycrest may conduct periodic audits electronically of my access to and disclosure of Confidential Information in order to monitor my compliance with the Policies.

8. I understand and acknowledge that as a condition of being a Baycrest employee, member of the medical staff, clinical or research fellow, student, independent contractor or volunteer, I may not disclose or access Confidential Information unless legally authorized to do so. I understand that a breach of this condition may be cause for suspension or termination of my employment, appointment or contract by Baycrest.

9. When my relationship with Baycrest ends or otherwise when requested by Baycrest, I will securely return all property to Baycrest, including keys, pass cards and any records of Confidential Information that are in my possession.

Date _____

_____ _____

Name and Title Department

_____

Signature

Title: Privacy Breach Protocol		
Date first created: May 2016	**Revised:**	**Approved By: Operations Committee**

1.0 Policy Statement:

A privacy breach happens whenever a person contravenes or is about to contravene a rule under the *Personal Health Information Protection Act, 2004* (PHIPA), the Baycrest Privacy, Confidentiality and Security of Information Policy or related privacy policies. The most obvious privacy breaches happen when an individual's information is lost, stolen or accessed by someone without authorization.

All privacy breaches must be reported immediately to the Chief Privacy Officer. If you have any questions about this policy, contact the Chief Privacy Officer. This policy is an appendix to the *Baycrest Privacy, Confidentiality and Security of Information Policy* and applies to all Baycrest Staff.

2.0 Background

Some examples of potential common privacy breaches include:

- A fax with an individual's information is misdirected to an unintended recipient.
- An unencrypted laptop with health information saved on the hard drive is stolen.
- A courier package of an individual's records is not delivered to the correct address.
- An unencrypted USB key with an individual's personal information is lost or stolen.
- An individual reads another individual's health record on a computer while waiting in a clinic room.
- A member of the Baycrest Staff talks about an individual with a friend who is not providing care to the individual.
- Health records to be disposed of are recycled and not shredded.
- A member of the Baycrest Staff reviews a neighbour's health record out of curiosity.
- A student or another member of the Baycrest Staff looks at health records on a self-initiated education project without being assigned to those individuals and without specific authorization for an approved educational exercise.
- Health information is given to the media without authorization.
- A member of the Baycrest Staff makes a copy of an ex-spouse's health record without the permission of the individual.

3.0 Definitions:

Baycrest: means collectively Baycrest Centre for Geriatric Care, Baycrest Hospital, The Jewish Home for the Aged, the Baycrest Day Care Centre, together with any affiliated departments or entities.

Baycrest Staff: means Baycrest employees, appointed medical staff, clinical and research fellows, scientists, students, volunteers and contractors who are given access to Confidential Information.

Confidential Information: has the same meaning as the term used in the *Baycrest Privacy, Confidentiality and Security of Information Policy*.

Patient: A registered patient of Baycrest Hospital or the Baycrest Day Care Centre. If the patient has a substitute decision-maker (SDM), references to the Patient in this Policy shall apply to the SDM where applicable.

Personal Health Information: has the same meaning as the term used in the *Baycrest Privacy, Confidentiality and Security of Information Policy*.

Resident: A registered resident of the Apotex (The Jewish Home for the Aged) or the Terraces. If the Resident has a substitute decision-maker, references to the Resident in this Policy shall apply to the SDM where applicable.

4.0 Procedure: Privacy Breach Protocol

The following steps will be taken by the Chief Privacy Officer if it is suspected that there has been a privacy breach.

4.1 Step One: Respond immediately by implementing the privacy breach protocol

a) Ensure appropriate Baycrest Staff are immediately notified of the breach, including the Chief Privacy Officer and the health care provider(s) whose Patients/Residents are potentially affected by the privacy breach.

b) Address the priorities of containment and notification as set out in the following steps.

4.2 Step Two: Containment – Identify the scope of the potential breach and take steps to contain it

a) Retrieve the hard copies of any Personal Health Information that has been disclosed.

b) Ensure that no copies of Personal Health Information have been made or retained by the individual who was not authorized to receive the information and obtain the person's contact information in the event that follow-up is required.

c) Determine whether the privacy breach would allow unauthorized access to any other Personal Health Information (e.g. an electronic information system) and take whatever necessary steps are appropriate (e.g. change passwords, identification numbers and/or temporarily shut down a system).

d) Consider notifying the Information and Privacy Commissioner of Ontario and/or legal counsel if appropriate.

e) Where applicable, notify external organizations of the breach as per data sharing agreements.

4.3 Step Three: Notification – Identify those individuals whose privacy was breached and notify them of the breach

a) At the first reasonable opportunity, any affected individuals will be notified.

b) The type of notification will be determined based on the circumstances (such as the sensitivity of the Personal Health Information, the number of people affected, and the potential effect the notification will have on the Patient(s)/Resident(s)).

For example, notification may be made by telephone or in writing, or in limited circumstances, a notation made in the Patient's/Resident's file to be discussed at his/her next appointment. (Note: Please seek the advice of the Chief Privacy Officer if relying on the notation option.)

c) Provide details of the extent of the breach and the specifics of the Personal Health Information at issue.

d) Advise affected individuals of the steps that have been or will be taken to address the breach, both immediate and long-term.

e) Consider engaging the Information and Privacy Commissioner of Ontario, legal counsel and Baycrest's insurer, as appropriate.

4.4 Step Four: Investigation and Remediation

a) Conduct an internal investigation into the matter. The objectives of the investigation will be to:
   - Ensure the immediate requirements of containment and notification have been addressed.
   - Review the circumstances surrounding the breach (include appropriate Baycrest Staff in the review process, including Human Resources if applicable).
   - Review the adequacy of existing policies and procedures in protecting Personal Health Information.
   - Address the situation on a systemic basis.
   - Identify opportunities to prevent a similar breach from happening in the future.

b) Change practices as necessary.

c) Ensure Baycrest Staff are appropriately re-educated and re-trained with respect to compliance with the privacy protection provisions of PHIPA and the circumstances of the breach and the recommendations of how to avoid it in the future.

d) Continue notification obligations to affected individuals as appropriate.

e) Consider engaging the Information and Privacy Commissioner of Ontario, legal counsel and Baycrest's insurer, as appropriate.

f) Human Resources to consider any disciplinary consequences for Baycrest Staff that follow from the privacy breach. Consider any contract issues in the case of independent contractors.

5.0 Reference Policies/Documents

Appropriate Use of Internet, E-mail, Electronic Devices
Appropriate Use of Mobile Devices
Code of Conduct
Confidentiality of Health Information
Health Information Protection Program
Personal Health Information Policy
Privacy Code
Privacy, Confidentiality and Security of Information Policy

Information and Privacy Commissioner of Ontario, What to Do When Faced with a Privacy Breach? Guidelines for the Health Sector: https://www.ipc.on.ca/images/Resources/up-hprivbreach.pdf.