Information
and Privacy
Commissioner/
Ontario

Report of the Information & Privacy Commissioner/Ontario

Review of the London Health Sciences Centre in Respect of the Ontario Joint Replacement Registry (OJRR):

A Prescribed Person under the *Personal Health Information Protection Act*

Ann Cavoukian, Ph.D.
Commissioner
October 2005

Review of the London Health Sciences Centre in Respect of the Ontario Joint Replacement Registry (OJRR):
A Prescribed Person under the *Personal Health Information Protection Act*

The *Personal Health Information Protection Act, 2004* (*PHIPA*) came into effect on November 1, 2004. The Information and Privacy Commissioner of Ontario (IPC) has been designated as the oversight body responsible for ensuring compliance with *PHIPA*. *PHIPA* establishes rules for the collection, use and disclosure of personal health information by health information custodians that protect the confidentiality of, and the privacy of individuals with respect to, that personal health information. In particular, *PHIPA* provides that health information custodians may only collect, use and disclose personal health information with the consent of the individual to whom the personal health information relates or as permitted or required by *PHIPA*.

Responsibilities of Prescribed Persons

Section 39(1) (c) of *PHIPA* permits health information custodians to disclose personal health information without consent to certain prescribed persons who compile or maintain registries for purposes of facilitating or improving the provision of health care or that relate to the storage or donation of body parts or bodily substances (prescribed persons).

Section 13(2) of Regulation 329/04 to *PHIPA* requires each prescribed person to have in place practices and procedures to protect the privacy of the individuals whose personal health information it receives and to maintain the confidentiality of that information. Section 13(2) further requires each prescribed person to ensure that these practices and procedures are approved by the IPC prior to November, 1, 2005, in order for health information custodians to be able to disclose personal health information to the prescribed person without consent and for the prescribed person to:

- be able to collect personal health information from health information custodians;
- use personal health information as if it were a health information custodian for purposes of section 37(1)(j) or section 37(3) of *PHIPA*; and
- disclose personal health information as if it were a health information custodian for purposes of sections 44, 45 and 47 of *PHIPA*.

Further, section 13(3) of Regulation 329/04 to *PHIPA* requires prescribed persons to make publicly available a plain language description of the functions of the registry, including a summary of the practices and procedures to protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information.

Mandate of the IPC with Respect to Prescribed Persons

Prescribed persons must ensure that their practices and procedures to protect the privacy of individuals whose personal health information they receive and to maintain the confidentiality of that information are reviewed and approved by the IPC prior to November 1, 2005.

Review Process

The IPC met with all of the prescribed persons to outline the process that would be followed by the IPC for the review of these practices and procedures. The process was to include a review of documentation relating to the practices and procedures of the prescribed person to protect the privacy of the individuals whose personal health information it receives and to maintain the confidentiality of that information, as well as a visit to the primary site where personal health information was held by the prescribed person. The IPC provided the prescribed persons with a preliminary checklist of privacy and security measures that the IPC would be looking for during the course of its review. The checklist included the following:

Human Resources

- Confidentiality agreements
- Disciplinary procedures for violations
- Clearly defined roles and responsibilities
- Appointed contact persons for privacy and security
- Ongoing education and training program for all staff, employees, affiliates, volunteers, etc. on security and privacy policies and procedures
- Third party agreements (with health information custodians, researchers, etc.)

Privacy

- Privacy policies and procedures that describe how the organization adheres to each fair information practice
- Privacy brochure – available upon request to the public
- Privacy Impact Assessments – for programs/database holdings
- Internal/external privacy audits
- Privacy crisis management protocols
- Data linkage protocols
- Procedures for de-identifying data

- Retention schedules and disposal procedures
- Inventory of all data holdings of personal health information
- Protocol for reviewing proposals in terms of their privacy impacts
- Mechanism for reviewing and updating privacy policies and procedures

Security

- Comprehensive security program including physical, technical and administrative measures
- Access control procedures – authentication and authorization
- Perimeter control
- Electronic access control
- Secure transfer procedures
- Audit trails
- Internal/external security audits
- Disaster Recovery Plan
- Mechanism for reviewing and updating security policies and procedures

The prescribed persons were informed that they were required to implement privacy and security measures and safeguards commensurate with the nature of the work undertaken by the prescribed person, the amount and sensitivity (e.g., level of identifiability) of the information in the custody and control of the prescribed person and the number and nature of the individuals who have access to personal health information. The scope of the review was to include practices and procedures relating to personal health information included in the specific registry associated with the prescribed person under section 13(1) of Regulation 329/04.

A site visit was to be scheduled within one month of the IPC receiving the documentation from the prescribed person. The purpose of the site visit was to provide the prescribed person with an opportunity to provide additional information to the IPC and to clarify their practices and procedures, and to provide the IPC with an opportunity to:

- Review the physical, technological and administrative security measures implemented;
- Ask questions about the documentation provided; and
- Discuss privacy and security matters with appropriate staff of the prescribed person.

Following the document review and site visit, each prescribed person was to be informed of any action that it needed to take prior to having its practices and procedures approved by the IPC.

Once all necessary action had been taken or if no action was necessary, the IPC would prepare a draft report that would be submitted to the prescribed person for review and comment. If the IPC was satisfied that the prescribed person had implemented practices and procedures that were sufficient to protect the privacy and confidentiality of personal health information, a letter of approval would be issued prior to November 1, 2005.

Description of the Prescribed Person

The London Health Sciences Centre is a public hospital within the meaning of the *Public Hospitals Act* that is comprised of the University Hospital, Victoria Hospital and South Street Hospital in London, Ontario and therefore, with respect to a majority of its functions, is a health information custodian within the meaning of section 3(1) of *PHIPA*. However, in respect of the Ontario Joint Replacement Registry (OJRR), the London Health Sciences Centre is a prescribed person for purposes of section 39(1) (c) of *PHIPA*.

As a result, in the course of conducting its review pursuant to section 13(2) of Regulation 329/04 to *PHIPA*, the IPC reviewed the privacy and security practices and procedures implemented by the London Health Sciences Centre in its capacity as a prescribed person pursuant to section 39(1) (c) of *PHIPA* and not the privacy and security practices and procedures implemented in its capacity as a health information custodian pursuant to section 3(1) of *PHIPA*.

The London Health Sciences Centre in respect of the OJRR collects personal health information about individuals requiring total hip or knee replacement surgery from participating orthopaedic surgeons in the Province of Ontario. Personal health information is not collected directly from the clinical record unless required for quality assurance (e.g., where personal health information is incomplete or incorrect). Additionally, one year after total hip or knee replacement surgery, personal health information is collected directly from the individual only if the individual consents to participate in the survey.

Personal health information is collected and used by the London Health Sciences Centre in respect of the OJRR to provide advice to the Ontario Ministry of Health and Long-Term Care (MOHLTC), to improve health care provided to individuals requiring total hip or knee replacement, to provide timelier access to total hip and knee replacement and to reduce re-operation rates and complications.

From the time it was established in April 2000 until July 1, 2005, the London Health Sciences Centre in respect of the OJRR collected personal health information with the express written consent of the individual to whom the information related. Beginning on July 1, 2005, express consent is no longer obtained. Individuals requiring total hip or knee replacement are provided with a "Patient Information Document" that outlines the:

- Types of personal health information disclosed to the OJRR;
- Purposes for which personal health information is collected, used and disclosed; and

- Mechanism by which individuals can contact their orthopaedic surgeon or the OJRR if they do not want their personal health information disclosed to the OJRR.

The Managing Director of the OJRR advised that, effective March 31, 2006, the OJRR will be dissolved. As a result, the London Health Sciences Centre in respect of the OJRR stopped collecting personal health information from individuals requiring total hip or knee replacement on September 30, 2005. However, until March 31, 2006, it will continue to collect personal health information from individuals who consented to participate in a survey one year after total hip or knee replacement and will continue to use personal health information in the OJRR.

Review of the Prescribed Person

Documents Reviewed

The London Health Sciences Centre in respect of the OJRR provided the IPC with a binder of documents on August 31, 2005 and with further documents on September 21, 2005, including:

Human Resources Materials

- Human Resources Policy on Employment Relationship
- Human Resources Policy on Confidentiality Agreements
- Human Resources Policy on Appointed Persons for Privacy and Security
- Human Resources Policy on Ongoing Education and Training on Privacy and Security
- Human Resources Policy on Surgeons Terminating Their Relationship with the OJRR
- Employee Pledge of Confidentiality for the OJRR
- Privacy and Confidentiality Agreement for the London Health Sciences Centre

Privacy Materials

- OJRR Privacy Code
- Privacy Brochure of the OJRR
- OJRR Poster Provided to Orthopaedic Surgeons
- Patient Information Document (Version 3.0)
- Communication Policy on Patient Consent for Data Submission
- Communication Policy on Media Requests for Information

- Privacy Audit Process
- Privacy Crisis Management Process and Documentation
- Consent Form (used prior to July 1, 2005)
- Confidentiality Policy of the London Health Sciences Centre (GEN022)
- Privacy Impact Assessment for the OJRR
- Data Flow Diagrams for the OJRR
- Data Collection at Decision and Surgery Diagrams
- OJRR Processes for Collection, Use and Disclosure of Personal Information
- Privacy and Confidentiality Self Learning Program for Regulated Health Professionals
- Scenario Based Learning for Regulated Health Professionals

Security Materials

- Security Policy on Physical, Technical and Administrative Data Security
- Security Policy on Audit Trails
- Security Policy on Data Validation
- Security Policy on Access to Data
- Security Policy on Subpoena or Court Order for Data
- Security Policy on Disaster Recovery Plan
- Security Policy on Termination of the OJRR

Third Party Agreements

- Third Party Researcher Pledge of Confidentiality for the OJRR
- Subcontractor Pledge of Confidentiality for the OJRR
- Surgeons Participation Agreement
- Agreement of Confidentiality and Non-Disclosure with Third Party Contractor

Other Documents

- Documentation relating to the length of time personal health information will continue to be collected and used prior to the dissolution of the OJRR
- Transitional matters that must be addressed prior to the dissolution of the OJRR

The IPC requested revisions to some of the above-mentioned documentation. The revised documentation was submitted on September 30, 2005.

Site Visit

IPC representatives conducted a site visit at the OJRR on September 26, 2005.

IPC met with the Managing Director of the OJRR, the Privacy Officer for the OJRR, the Privacy Officer for the London Health Sciences Centre, the Computer Applications and Webmaster Specialist of the OJRR and the Coordinator for Information Management at the London Health Sciences Centre. Discussions focused on the following topics:

- Decisions made with respect to the retention, transfer or disposal of personal health information in the OJRR upon its dissolution;
- Continued collection and use of personal health information until dissolution;
- Procedures for the use and disclosure of personal health information for research;
- Procedures related to the retention and disposal of personal health information; and
- The documentation provided to the IPC.

A site visit to the data centre where the OJRR is located was also conducted.

Findings of the Review

Human resources

In addition to the Privacy Officer appointed by the London Health Sciences Centre in its capacity as a health information custodian pursuant to section 3(1) of *PHIPA*, a Privacy Officer has also been appointed by the London Health Sciences Centre in its capacity as a prescribed person pursuant to section 39(1) (c) of *PHIPA*.

The Privacy Officer appointed in its capacity as a prescribed person pursuant to section 39(1) (c) of *PHIPA* is accountable to the Managing Director of the OJRR and is responsible for investigating and resolving breaches of privacy and for establishing, implementing and improving privacy and security practices and procedures. A Sub-Committee on Consent and Confidentiality has also been established to make recommendations to the Advisory Committee of the OJRR on issues of privacy and confidentiality.

Prior to the commencement of employment or placement as the case may be, every employee, student, volunteer and agent of the London Health Sciences Centre and every member of the Advisory Committee and Sub-Committee on Consent and Confidentiality is required to sign a Pledge of Confidentiality and a Privacy and Confidentiality Agreement. By signing the Pledge of

Confidentiality and the Privacy and Confidentiality Agreement, these individuals acknowledge that a breach of the Pledge of Confidentiality or the Privacy and Confidentiality Agreement may result in sanctions up to and including termination of employment or termination of placement.

In the event that the London Health Sciences Centre will continue to collect, use or disclose personal health information in the OJRR after March 31, 2006, the Pledge of Confidentiality and the Privacy and Confidentiality Agreement should be amended to reference *PHIPA*, to reference and define personal health information and to require employees, students, volunteers and agents of the London Health Sciences Centre and members of the Advisory Committee and Sub-Committee on Consent and Confidentiality, to:

- Acknowledge that they have read, understand and will agree to comply with the privacy and security practices and procedures implemented by the London Health Sciences Centre;
- Agree that they will not use personal health information for any purpose other than the purpose for which access was given unless permitted or required by law and that they will not disclose personal health information except as permitted or required by law; and
- Immediately notify the London Health Sciences Centre upon becoming aware of a breach of the Pledge of Confidentiality and Privacy and Confidentiality Agreement.

In addition, at the commencement of employment or placement, every employee, student, volunteer and agent of the London Health Sciences Centre receives privacy training and orientation on the practices and procedures implemented to protect the privacy of individuals whose personal health information is contained in the OJRR and to maintain the confidentiality of that information.

It is recommended that if the London Health Sciences Centre continues to collect, use or disclose personal health information in the OJRR after March 31, 2006, that a comprehensive program for ongoing privacy and security training for all employees, students, volunteers and agents be developed that extends beyond initial orientation and training and that the details of this privacy and security training be forwarded to the IPC for review prior to implementation.

Privacy

The London Health Sciences in respect of the OJRR has developed a privacy code in accordance with the ten fair information practices set out in Schedule 1 to the *Personal Information Protection and Electronic Documents Act*. It has also developed a brochure that describes the OJRR, the types of personal health information collected, from whom and the manner in which personal health information is collected, the purposes for which the personal health information is used and disclosed and the process by which an individual can withhold or withdraw consent to the disclosure of personal health information to the OJRR.

The OJRR Privacy Code and OJRR Privacy Brochure are available on the OJRR website, as is the Privacy Impact Assessment conducted in 2005 by an independent third party consultant.

A poster has also been developed for the offices of participating orthopaedic surgeons aimed at advising individuals requiring total hip or knee replacement of the existence of the OJRR. In addition, a "Patient Information Document" is provided to all individuals requiring total hip or knee replacement surgery through participating orthopaedic surgeons that outlines the types of personal health information collected, the purposes for which it is collected, used and disclosed and the mechanism by which individuals can "opt out" of having their personal health information disclosed to the London Health Sciences Centre in respect of the OJRR.

In the event that individuals do not want their personal health information disclosed to the London Health Sciences Centre in respect of the OJRR, only de-identified wait time information will be disclosed by orthopaedic surgeons. Further, in the event that individuals decide at a later date that they do not want their personal health information to be contained in the OJRR, their personal health information is destroyed.

The London Health Sciences Centre has also implemented a procedure for responding to breaches of privacy with respect to the OJRR which addresses containment, notification and measures to ensure similar breaches do not occur in future. However, a procedure has not been developed for responding to complaints or inquiries from the public with respect to the practices and procedures implemented to protect the privacy of individuals whose personal health information is collected and to maintain the confidentiality of that information.

It is recommended that in the event that the London Health Sciences Centre continues to collect, use or disclose personal health information in the OJRR after March 31, 2006, that a procedure for responding to complaints or inquiries from the public is developed and that this procedure be forwarded to the IPC for review and comment.

The London Health Sciences Centre protects the privacy of individuals whose personal health information it collects with respect to the OJRR and maintains the confidentiality of that information in a number of ways.

Access to personal health information is limited according to functional level of need. Participating orthopaedic surgeons are only permitted to access personal health information of their own patients and not that of patients of other orthopaedic surgeons. Field Co-ordinators, who are agents of the London Health Sciences Centre and who are responsible for validating, correcting and inserting missing personal health information, only have access to the personal health information of individuals in their respective region. Only five individuals (all employees of the London Health Sciences Centre) have access to all personal health information in the OJRR.

Third parties retained by the London Health Sciences Centre who require or may have access to personal health information in the OJRR must sign a Subcontractor Pledge of Confidentiality and an Agreement of Confidentiality and Non-Disclosure prior to the commencement of services. By signing the Subcontractor Pledge of Confidentiality and Agreement of Confidentiality and Non-Disclosure, third parties acknowledge that the failure to maintain privacy may result in consequences up to and including contract termination.

In the event that the London Health Sciences Centre will continue to collect, use or disclose personal health information in the OJRR after March 31, 2006, it is also recommended that the Subcontractor Pledge of Confidentiality and Agreement of Confidentiality and Non-Disclosure be amended to reference *PHIPA*, to reference and define personal health information and to require third parties to:

- Comply with the privacy and security practices and procedures implemented by the London Health Sciences Centre in respect of the OJRR;
- Prohibit employees or persons acting on their behalf from accessing personal health information unless they have agreed to comply with the Subcontractor Pledge of Confidentiality and Agreement of Confidentiality and Non-Disclosure;
- Not use the personal health information for any purpose other than the purposes for which they were provided access unless permitted or required by law and to not disclose personal health information except as permitted or required by law; and
- Immediately notify the London Health Sciences Centre upon becoming aware of a breach of the Subcontractor Pledge of Confidentiality and Agreement of Confidentiality and Non-Disclosure.

The London Health Sciences Centre does not use or disclose personal health information in the OJRR for research purposes. Further the London Health Sciences Centre does not disclose information to the MOHLTC or publish information that either alone or in combination with other information could reasonably identify the individual to whom the information relates. No information is published in cell sizes of less than five aggregated records.

It is recommended that prior to the use or disclosure of personal health information in the OJRR for research, practices and procedures be developed relating to the use and disclosure of personal health information for research that are consistent with *PHIPA* and its regulations. It is also recommended that the Pledge of Confidentiality with Third Party Researchers be amended to require researchers to comply with section 44(6) of *PHIPA* and to set conditions and restrictions related to the use, disclosure, security, return and disposal of personal health information pursuant to section 44(5). Further, it is recommended that these documents be forwarded to the IPC for review and comment prior to the use and disclosure of personal health information for research.

As the Ontario module for the Canadian Joint Replacement Registry, the London Health Sciences Centre in respect of the OJRR discloses personal health information to the Canadian Institution for Health Information, a prescribed entity under section 45(1) of *PHIPA*, which maintains and compiles the Canadian Joint Replacement Registry. It also discloses personal health information to the Institute for Clinical Evaluative Sciences, another prescribed entity under section 45(1), for purposes of analysis or compiling statistical information with respect to the management, evaluation, monitoring, allocation of resources or planning for all or part of the health system. These disclosures are permitted by section 13(5) of Regulation 329/04 to *PHIPA*.

Security

The London Health Sciences Centre in respect of the OJRR has a security program that incorporates physical, technical and administrative security measures.

Access to the OJRR offices is controlled by security cards. All personal health information is stored in locked file cabinets. The OJRR database is located in two servers at a physically secure data centre with security card access and video camera surveillance. Administration and maintenance of the OJRR database is provided by employees of the London Health Sciences Centre who sign a Pledge of Confidentiality and Privacy and Confidentiality Agreement. A disaster recovery plan has also been developed and implemented.

Personal health information is, for the most part, collected from participating orthopaedic surgeons electronically either through the use of handheld computers or personal computers that transmit personal health information via the Internet using 128 bit encryption to a dedicated web server with a firewall system or through direct entry of personal health information onto the dedicated web server. A username and password are required for access to the dedicated web server. Personal health information is immediately transferred from the dedicated web server to a database that resides on a separate server that is password controlled and that stores user identifications in an encrypted manner.

Access to the handheld computers is protected by a user name and password and has software that automatically verifies the user name and password, encrypts personal health information and erases personal health information if the battery is removed or if an unauthorized individual attempts to access personal health information. Similarly, the program on personal computers that accesses the OJRR is password and username protected and the database is encrypted on the hard drive of the personal computer which renders the personal health information meaningless in the event that the database is copied from the hard drive of the personal computer.

In the event that a participating orthopaedic surgeon wishes to disclose personal health information to the London Health Sciences Centre in respect of the OJRR in paper format, it is transferred using a bonded courier.

Audit logs are created for all internal and external accesses to personal health information in the OJRR however there is no policy or procedure for the review of audit logs on a frequent basis in order to identify, remedy and impose sanctions on those who access personal health information in the OJRR for unauthorized purposes. It is therefore recommended that prior to the dissolution of the OJRR on March 31, 2006, that a policy or procedure be developed for the review of audit logs setting out the frequency of the review and the person who will be responsible for conducting the review.

Although the London Health Sciences Centre has implemented a number of security measures, the IPC recognizes that the security of personal health information requires ongoing vigilance and a commitment to continuous improvement. Given the volume and sensitivity of personal health information contained in the OJRR, it is recommended that in the event that the London Health Sciences Centre continues to collect, use or disclose personal health information in the

OJRR after March 31, 2006, that a more comprehensive and systemic information security management program should be implemented. This should include a comprehensive threat and risk assessment (TRA), preferably carried out by an independent party, that identifies all external and internal risks to privacy in order to provide a strong basis for prioritizing those risks and developing an action plan to mitigate those risks.

Further, the London Health Sciences Centre has not developed or implemented a policy relating to the retention and disposal/destruction of personal health information with respect to the OJRR. Prior to the dissolution of the OJRR on March 31, 2006, a policy for the retention and disposal/ destruction of personal health information should be developed and forwarded to the IPC for review and comment. This policy should specify how long personal health information on various media will be retained and when and how personal health information on various media will be disposed of/destroyed.

In addition, the London Health Sciences Centre has yet to make any decisions with respect to whether personal health information in the OJRR will be retained by the London Health Sciences Centre upon the dissolution of the OJRR on March 31, 2006, whether it will be transferred to another person (e.g., a health information custodian, a prescribed entity under section 45(1) of *PHIPA* or prescribed section 39(1) (c) person) or whether it will be disposed of by the London Health Sciences Centre. The decision with respect to the retention, transfer or disposal of personal health information in the OJRR, once made, should be communicated to the IPC.

Further, in the event personal health information will be transferred upon the dissolution of the OJRR on March 31, 2006, the London Health Sciences Centre should develop a procedure to ensure that personal health information in the OJRR is transferred in a secure manner and in accordance with the provisions of *PHIPA*. It should also develop a detailed conversion strategy, draft and execute any and all necessary agreements, and provide copies of these procedures, conversion strategies and agreements to the IPC for review and comment prior to the transfer of personal health information.

Summary of Recommendations

Major Recommendations

Based on the review of documentation and the site visit, there are no major recommendations that require rectification or resolution by the London Health Sciences Centre in respect of the OJRR prior to November 1, 2005.

Recommendations To be Acted Upon and Resolved Prior to March 31, 2005

Based on the review of the documentation and the site visit, the IPC is making the following recommendations that the London Health Sciences Centre in respect of the OJRR is required to act upon and resolve prior to March 31, 2006:

1. Develop and implement a formal policy or procedure for the regular review of audit logs in order to identify, remedy and impose sanctions on those who access personal health information in the OJRR for unauthorized purposes and that it be provided to the IPC for review and comment upon its completion.

2. Develop and implement a formal policy on the retention and disposal/destruction of personal health information which specifies how long personal health information on various media will be retained and when and how personal health information on various media will be disposed of/destroyed and forward this policy to the IPC for review and comment when it has been completed.

3. Advise the IPC when a decision has been made by the London Health Sciences Centre with respect to whether personal health information in the OJRR will be retained by the London Health Sciences Centre upon the dissolution of the OJRR on March 31, 2006, whether it will be transferred to another person (e.g., a health information custodian, a prescribed section 45(1) entity under *PHIPA* or prescribed section 39(1) (c) person) or whether it will be disposed of by the London Health Sciences Centre.

4. In the event personal health information will be transferred to another person upon the dissolution of the OJRR, develop and implement a procedure to ensure personal health information is transferred in a secure manner and in accordance with *PHIPA*. This procedure should be provided to the IPC for review and comment prior to any transfer of personal health information.

5. In the event that personal health information will be transferred to another person upon the dissolution of the OJRR, develop a detailed conversion strategy and draft and execute all necessary agreements. This conversion strategy and drafts of all agreements should be provided to the IPC for review and comment prior to any transfer of personal health information.

Other Recommendations

Based on the review of documentation and the site visit, the IPC is making the following recommendations that the London Health Sciences Centre in respect of the OJRR is not required to act upon/resolve unless it will continue to collect, use and disclose personal health information after March 31, 2006:

1. Amend the Pledge of Confidentiality and the Privacy and Confidentiality Agreement to include references to *PHIPA*, to reference and define personal health information and to include provisions requiring employees, students, volunteers and agents of the London Health Sciences Centre in respect of the OJRR and members of the Advisory Committee and Sub-Committee on Consent and Confidentiality, to:

(a) Acknowledge they have read, understand and agree to comply with the privacy and security practices and procedures implemented by the London Health Sciences Centre;

(b) Agree that they will not use personal health information for any purpose other than the purpose for which access was given unless permitted or required by law and that they will not disclose personal health information except as permitted or required by law; and

(c) Immediately notify the London Health Sciences Centre upon becoming aware of a breach of the Pledge of Confidentiality and Privacy and Confidentiality Agreement.

2. Develop and implement a comprehensive program for ongoing privacy and security training for all employees, students, volunteers and agents of the London Health Sciences Centre in respect of the OJRR and forward details of this program to the IPC when they are available and prior to implementation.

3. Develop and implement a procedure for responding to complaints or inquiries from the public with respect to the practices and procedures implemented by the London Health Sciences Centre to protect the privacy of individuals whose personal health information is contained in the OJRR and to maintain the confidentiality of that information and to forward the procedure to the IPC for review and comment prior to implementation.

4. Amend the Subcontractor Pledge of Confidentiality and the Agreement of Confidentiality and Non-Disclosure to include references to *PHIPA*, to reference and define personal health information and to include provisions requiring third parties to:

(a) Comply with the privacy and security practices and procedures implemented by the London Health Sciences Centre;

(b) Prohibit employees or persons acting on their behalf from accessing personal health information unless they have agreed to comply with the Subcontractor Pledge of Confidentiality and Agreement of Confidentiality and Non-Disclosure;

(c) Not use the personal health information for any purpose other than the purposes for which they were provided access unless permitted or required by law and to not disclose personal health information except as permitted or required by law; and

(d) Immediately notify the London Health Sciences Centre upon becoming aware of a breach of the Subcontractor Pledge of Confidentiality and Agreement of Confidentiality and Non-Disclosure.

5. In the event that the London Health Sciences Centre decides to use or disclose personal health information in the OJRR without consent for research, develop and implement practices and procedures relating to the use and disclosure of personal health information for research purposes that are consistent with *PHIPA* and its regulations. These practices

and procedures should be forwarded to the IPC for review and comment prior to the use or disclosure of personal health information for research.

6. In the event that the London Health Sciences Centre decides to use or disclose personal health information in the OJRR for research, amend the Pledge of Confidentiality with Third Party Researchers prior to any use or disclosure of personal health information for research in order to require researchers to comply with their responsibilities pursuant to section 44(6) of *PHIPA* and to set conditions and restrictions with respect to the use, disclosure, security, return and disposal of personal health information pursuant to section 44(5) of *PHIPA*.

7. Conduct regular comprehensive threat and risk assessments, with emphasis on both internal and external threats to security.

Statement of IPC Approval of Practices and Procedures

The IPC is satisfied that the London Health Sciences Centre in respect of the OJRR has in place practices and procedures that sufficiently protect the privacy of individuals whose personal health information it receives and to maintain the confidentiality of that information. Accordingly, effective October 31, 2005, the practices and procedures of the London Health Sciences Centre in respect of the OJRR have been approved by the IPC.