TAHSN RESEARCH ETHICS COMMITTEE (LIMITED TERM)

PRINCIPLES FOR DEVELOPMENT OF POLICY and GUIDELINES ON SECURITY OF PERSONAL HEALTH INFORMATION USED FOR RESEARCH PURPOSES

Approved by TAHSN Research Committee - February 4th 2008

PREAMBLE

Ontario's health privacy law, the *Personal Health Information Protection Act*, 2004 (PHIPA) came into effect in November 2004. This law applies to all health information custodians (HICs), such as doctors, laboratories, pharmacies, and hospitals. It also applies to all researchers, consultants, staff, clinicians, students and volunteers working at organizations that collect, use and/or disclose personal health information (PHI).

The Toronto Academic Health Science Network (TAHSN) hospitals and the University of Toronto recognize the importance of respecting and protecting the privacy and confidentiality rights of patients and research subjects at all times. To ensure that these rights are upheld in the conduct of research involving the handling and/or use of personal health information (PHI) before, during and after use for research purposes, the following principles have been developed to facilitate the development by TAHSN member organizations of policies and guidelines relative to security of PHI in electronic and paper-based format used for research purposes. These principles continue to apply in those instances when health information is collected, used, or disclosed for various purposes, so long as research is one of those purposes, regardless of whether it is the dominant or primary purpose.

Although the attached Principles document focuses on PHI in electronic and paper-based formats, many of the principles may be applicable to other types and forms of data, including bio-informatics, personal information (as defined under the Freedom of Information and Protection of Privacy Act - FIPPA) and tissue samples. Audio, video, and other multimedia records that exist as electronic computer files should be treated in the same fashion as electronic files. Those that do not exist as electronic computer files should be treated in the same way as paper records.

The following principles reflect existing statutory and regulatory requirements, and are meant to supplement and complement existing legal, regulatory and accreditation requirements, including PHIPA and any applicable provincial or federal standards for health research. Each member of a research team shall comply with the obligations of its hospital (i.e. health information custodian – HIC) and, as required, the obligations imposed by relevant sponsors, peer-review funding agencies, governments, and law. TAHSN member organizations are responsible for monitoring compliance with this policy, consistent with their own existing internal procedures and processes. In addition, individual Research Ethics Boards may require additional safeguards and / or require individual research plans to adhere to more stringent requirements.

DEFINITIONS

"**data**" refers to all PHI, in any form which is, has been, or may be used for research and any related purposes - such as, recruitment, database creation, research project feasibility assessment, pilot study, and research planning and follow-up. This includes de-identified PHI, and should be read to go beyond the scope of the definition of PHI provided herein.

"**de-identification"** means a method of ensuring that information does not identify an individual, and where there is no reasonable basis to believe that the information could be used on its own or combined with information available elsewhere to identify an individual.

"disclosure" refers to the release of identifiable PHI in respect of a particular individual outside of the specified Research Ethics Board-approved research plan team members, including release to anyone or any entity outside of the HIC.

"**disposal**" means appropriate steps to dispose of PHI in a manner that prevents subsequent use and / or reconstruction of the record, data and / or information.[1]

"**encryption**" means the electronic processing of data using the HIC's approved algorithm for encryption that results in the data not being understandable without a password or key.

"**most responsible researcher**" (MRR) means the researcher responsible for that project, trial, or other endeavour at a site. This will be the person who received approval from the site REB to conduct that study.

"**personal health information**" has the same meaning set out in the *Personal Health Information Protection Act*, 2004 (PHIPA). PHIPA defines PHI as information about an individual that identifies a person, and connects them with their healthcare. Examples of PHI include (but are not limited to) all unique identifiers (including health care number), the identity of a substitute decision maker, information concerning payments for healthcare, eligibility for payments status, all treatment and diagnostic information and family health history. This includes personal health information that originates in PHI databases as well as PHI from outside of Ontario, Canada, and/or pertains to an individual without status.

"**research**" means a systematic investigation designed to develop or establish principles, facts or generalizable knowledge, or any combination of these, and includes the development, testing and evaluation of research as well as the identification of potential research study participants.[2]

"**Research Ethics Board**" means a board of persons that is established for the purpose of approving research plans under section 44 of PHIPA and that meets the prescribed requirements.[3]

"**retention and storage**" refer collectively to information management practices associated with the (a) maximum and minimum length of time determined by legal and regulatory requirements and (b) method of holding a given piece of information and / or records securely.

"**transfer**" refers to the meaningful hand-off of accumulated PHI for research purposes to another researcher. This process may or may not require a reasonable effort to give notice to the individuals to whom the records relate prior to transfer.

PRINCIPLES

Overarching Principle

Researchers are to work with de-identified data at all times.

If it is not possible in the context of the research to work with de-identified data and if use of identifiable data has been approved by the HIC's REB:

for electronic data

[1] Guide to the Ontario Personal Health Information Protection Act. p.455.

[2] *Personal Health Information Protection Act,* 2004, (PHIPA), s.2. Available online at http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/04p03_e.htm#BK5.

[3] *Personal Health Information Protection Act,* 2004, (PHIPA), s.2. Available online at http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/04p03_e.htm#BK5.

- data are to be used in a secure server environment or via remote (including VPN) access to a secure server environment; or, if this is not possible,
- data are to be encrypted.

for paper-based data

- paper should be avoided whenever possible as a medium for storing PHI for research or for research-related purposes.
- data are to be used in a secure HIC environment with restricted access and lockup capability; or, if this is not possible
- data are to be handled as per established HIC policies

Accountability

HICs are to:

- provide a secure data environment and to make tools available to researchers to ensure security of data in and out of that environment (e.g. encryption tools, VPN access, privacy and security educational training). Appendix 1 may be used by HICs to ensure that their server environments would be deemed secure.
- ensure that every approved research study has one continuously staffed role (usually the MRR) accountable to the HIC and REB of record for data privacy and security through all phases of a research study (from initial request for approval through to collection and final archiving / destruction of data).
- have policies and procedures in place to ensure responsible and secure transfer of data from one individual to another (e.g. from one MRR to another or from one organization to another)
- establish data security protocols relative to portable devices and paper records.
- discourage paper collection of PHI whenever possible
- provide education and training regarding HIC policies and privacy requirements to all researchers working with data, as well as to Research Ethics Board (REB) members and other appropriate constituencies.
- consider establishing and maintaining a compliance monitoring or audit function.
- appoint a "responsible person" to implement policy requirements where no MRR or approved research plan may be connected to a given set of data amassed for research purposes. These assigned datasets are to be maintained and used in accordance with policy.

Most Responsible Researchers are to:

- maintain a research log (to the standard set by the HIC) during and after the study, documenting all security measures and privacy protection measures that are applied including administrative, technical and physical safeguards.
- be personally accountable for information management for their respective research studies, using the tools made available, or recommended, by the institution.
- be responsible for local security of data and vulnerable devices, and reporting of losses and security incidents as soon as possible
- ensure compliance with data security and privacy practices within their research teams and by colleagues.

REBs are to:

- ensure that a harmonized privacy risk assessment forms part of the REB submission and protocol renewal process. The assessment is to be sufficiently detailed to capture particulars of complexity and relative risk to data security (e.g. multiple researchers, multiple institutions, identifiable data, small cell factors, sharing of data, transfer of data, out-of-country movement of data, long-term research issues). Appendix 2 may be used by REBs as part of the protocol submission process until the TAHSN Human Subjects Research Application form (or similar application form) has been revised to address the privacy risk issue.
- determine in the REB approval process when identified data may be used in the course of a research project. HICs may wish to consider requiring REBs to establish a list of such projects for monitoring and risk management purposes.

All Members of the Research Team

- It is the responsibility of all members of a research team to fully familiarize themselves with all protocol requirements (including privacy requirements), to follow them, and to promptly report incidents (including loss, theft, or lack of compliance with data security requirements) to the relevant REB, so that remedial and corrective actions may be initiated.

Principles for Each Phase of Research

Phase	Principle	Electronic Data	Non-Electronic Data
Collection	• Appropriate consent for use of data for research is to be obtained where applicable. • Data are to be de-identified at as early a stage as practical. • Data may be de-identified once the cohort of interest is created (i.e. linked), but before the research project is begun (e.g. lab results liked to a hospitalization of interest). • The keys / codes for identification of de-identified data are to be securely stored separate from the de-identified data. Access to the keys / codes is to be limited to the MRR or official designate. Where sensitivity or privacy is required, data keys may be held by a delegated third party not directly related with analysis. • If identifiable data are needed, documented justification for this is required as part of the REB submission. • The minimum amount of identified data required to practically conduct the research should be authorized in advance in writing. Documented justification is required for the collection of each of these data elements as part of the REB submission. • Data sets collected under the authority of an approved REB protocol are to be securely archived upon expiry of the REB approval.		o Wherever possible, paper should be avoided as a medium for collection of PHI for research or for research related purposes. If health information must be recorded or retained on paper, then it should be de-identified if at all possible. o Paper-based data collection should be done under a unique study number with maintenance of a secured 'key' to the nominal data, health card or medical record number. o Whenever practicable, consideration should be given to transferring paper-based information to electronic media and storing on a secure central server, instead of on paper, so that automated methods may be used to back-up and limit access to the information, and to track and audit use and disclosure of the information. o Original PHI records and copies of PHI records must never leave the premises of the HIC except through the approved HIC process for doing so.
Use	• Use only de-identified data wherever possible. Identifiable data is to be used only when no other option is practical. • Data are to be de-identified as early as possible. • The number of people able to access both identifiable and de-identified data is to be limited to the smallest number practicable, with links between identifiers and de-identified data stored separately and only in a secured environment.	o If using identifiable data outside a secure server environment, the data are to be encrypted using methods approved by the HIC as quickly as possible as institutional resources to enable this are available. o Electronic data	o Wherever possible, paper should be avoided as a medium for use of PHI data for research or for research related purposes. . o Original PHI records and copies of PHI records must never leave the premises of the HIC except through an approved HIC process which specifically address risks of loss or theft.

Phase	Principle	Electronic Data	Non-Electronic Data
	• A log identifying approved levels of access for researchers involved in a study is to be established and maintained throughout the study for audit purposes. • Researchers and their designated staff who have access to identified and/or de-identified data are to sign confidentiality / non-disclosure agreements. • MRRs and REBs are to be vigilant of situations in which data linkage could result in identification of data – this includes linkage with publicly available databases as well as those available within the HIC or to the researcher(s) working with the data. • Data should be used only in a secure HIC environment (such as, a secure server) that has appropriate technical and physical safeguards compliant with HIC IT security policies, and which are maintained, updated, and monitored on a regular basis. • Following the expiry of approval, further use of data collected for research purposes is not permitted without approval of the institution or subsequent REB approval.	should not be downloaded from a secure server to a non-secured device for use and/or storage unless data are encrypted using methods approved by the HIC as quickly as possible as institutional resources to enable this are available.	o Identifiable data is to be used in a secure HIC environment with restricted access and lockup capability; or, if data must be used in a non-secure research environment, it must be appropriately blinded or de-identified. o Electronic data should not be downloaded from a secure server and printed. Electronic data that is printed is to be used in a secure HIC environment with restricted access and lockup capability; or, if data must be used in a non-secure research environment, it must be appropriately blinded or de-identified.
Disclosure	• Researchers may disclose only de-identified data unless otherwise required by law or as consented to by a study subject. The rules for HICs relative to disclosure may be different than those for researchers. • Secondary or other disclosure of data requires additional REB disclosure and review prior to approval. For example, PHI transmitted to the United States may be subject to the USA Patriot Act 2001. • Disclosure of PHI to a researcher external to the Institution/HIC requires consent of the patient or approval of the REB at the disclosing Institution / HIC.	o If disclosing identifiable data outside a secure server environment, the data are to be encrypted using methods approved by the HIC as quickly as possible as institutional resources to enable this are available. o Electronic transfer of identifiable data (e.g. via e-mail) should not occur.	o If disclosing identifiable data outside a secure environment, the data are to be handled as per high security standards set by the HIC, in order to prevent unauthorized access and disclosure risk. o Removal, transmission, and transportation of identifiable paper-based data are to follow high security standards as set by the HIC, in order to prevent unauthorized access and disclosure risk.
Retention & Storage	• The MRR (under the direction of the principal investigator) is responsible for placing data on a secure HIC server environment and ensuring that it is not removed from that environment unless the appropriate administrative, technical and physical safeguards are in place.	o The HIC managing the secure server is responsible for ensuring data security and backup, and provision of agreed upon resources to	o Wherever possible, paper should be avoided as a medium for retention and storage of PHI data for research or research related purposes. o Paper-based PHI should only be retained as long as is

Phase	Principle	Electronic Data	Non-Electronic Data
	• Length of time for retention of data beyond a study's approved active phase is to comply with current standards, and when practical, should be clearly defined. • Data should be stored only in a secure institutional / HIC server or research environment that has appropriate technical and physical safeguards, consistent with HIC security policies, and which are maintained and updated on a regular basis.	researchers relative to these responsibilities, having regard to the need to be able to access the information during the entire retention period.	necessary to fulfill the approved purposes of the retention.
Disposal	• HICs are to have policies and procedures in place to ensure that data are flagged for disposal once stored for the required length of time. • HICs are to have policies, procedures, and tools in place to ensure secure disposal of data, both electronic and non-electronic – with review of these standards held on a regular basis. • HIC researchers are to inform relevant REB(s) when responsibility for data is transferred to another MRR or destroyed using the appropriate secure destruction procedures.	o HICs are to provide researchers with agreed upon resources to ensure proper disposal of data from endpoint and portable devices (e.g. laptops, PDAs, USB keys, CDs, desktop PCs).	o At the end of the approved retention period, the PHI records should be securely destroyed (e.g. cross-cut shredding) in such a way that the information is not recoverable.

EDUCATION AND TRAINING

Education and training regarding the HIC's policies and privacy requirements are to be provided to all researchers working with data, as well as to Research Ethics Boards (REB) and other appropriate constituencies. This process is the responsibility of the institution where the research is taking, or will take, place.

ENFORCEMENT

Information management practices associated with PHI used for research purposes are subject to applicable legal, regulatory, accreditation and policy requirements. Principle enforcement considerations include:

- PHIPA ensures accountability by granting individuals the right to complain to the Information and Privacy Commissioner (IPC) about the practices of a healthcare organization, including research. It establishes remedies for breaches of the legislation, including fines per breach for an individual institution / member organization and for individuals within that institution / member organization.
- Other countries typically have privacy legislation that may pose additional requirements on international research. For example, the American *Health Insurance Portability and Accountability Act* (HIPAA) allows individuals to file a complaint within an organization, or through the Department of Health and Human Services Office of Civil Rights.
- TAHSN member organizations have existing Research Ethics Board (REB) processes for approving research plans. Inappropriate and / or unauthorized information management practices associated with research can be subject to redacted approvals, findings of misconduct, and / or findings related to protocol violations.

Contraventions of this policy may also lead to disciplinary action consistent with individual institution / member organization's employee / human resources misconduct policies.

RESOURCES

Personal Health Information Protection Act, 2004 (PHIPA)
- http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/04p03_e.htcm

CIHR Best Practices for Protecting Privacy in Health Research:
- http://www.cihr-irsc.gc.ca/e/documents/et_pbp_nov05_sept2005_e.pdf

US Dept of Health and Human Services
- http://www.hhs.gov/ocr/hipaa/

UHN *De-Identification of Personal Information* document

Non-technical guidelines re server security for storage of electronic personal health information (ePHI)
- http://www.cms.hhs.gov/SecurityStandard/Downloads/SecurityGuidanceforRemoteUseFinal122806.pdf
- http://www1.umn.edu/oit/security/serversecurity.html

Hospital for Sick Children Order – Order HO-004
- http://www.ipc.on.ca/index.asp?navid=53&fid1=7616

Interim Strategy for Protecting Personal Health Information in Response to IPC Order HO-004
- Prepared by the Toronto Central Local Health Integration Network Privacy Working Group / TAHSN Privacy Working Group (May 30, 2007)

Draft – November 1, 2007
Document prepared by: TAHSN Research Ethics Committee - Working Group on Security of Personal Health Information Used for Research Purposes

Working Group Members:

Leslie Bush	Assistant Vice-Provost, Health Sciences Sector, University of Toronto
Jodi Butts	Legal Council Mt Sinai Hospital and Member of the TAHSN Privacy Officer's Group
Kate Dewhirst	Legal Council CAMH
Rafael Eskenazi	Director of University of Toronto's Freedom of Information and Protection of Privacy Act (FIPPA) Office
Tracy Kosa	Privacy Office UHN
Wes Robertson	Director of Administrative Computing, Faculty of Medicine
Julie Spence	Chair, REB St. Michael's Hospital, Division of Emergency Medicine, Department of Medicine, University of Toronto
Rachel Zand	Director, Ethics Review Office at the University of Toronto

APPENDIX 1

FACTORS FOR IDENTIFYING A SECURE SERVER

The table below lists some of the most important factors to be considered when determining if a computer can be considered a "secure server" for the purpose of storing PHI. HICs may wish to use this as a checklist for review by their IT officers, privacy officers, and REBs. Due to the wide variety of server operating systems and hardware, specific security procedures and guidelines are necessarily much more detailed; however, a "no" answer to one or more of the following relatively generic questions will identify, for any server, a serious security vulnerability which must be addressed if it is to be used to store PHI.

#	Identifier	yes	no
1.	Is the server dedicated to the storage of non-public information?		
2.	Is the server administrated by a full-time information technology professional?		
3.	Are all account management and login activities logged, and regularly reviewed?		
4.	Are individually-named accounts, with strong passwords, created for each user?		
5.	Has the operating system's default "guest" account been deactivated?		
6.	Is the "administrator / root" account used only for actual system administration?		
7.	Are operating system patches installed on a regular (ideally automatic) basis?		
8.	Is anti-virus software installed, and set to automatically update on a daily basis?		
9.	Is a hardware or software firewall, or similar packet filtering software, in use?		
10.	Is the server located in a clean, physically secure, limited-access location?		
11.	Is there cooling available to keep the server within its rated heat specifications?		
12.	Is an uninterruptible power supply (UPS) in use to protect from power problems?		
13.	Have all unneeded services and ports (i.e. www, telnet, ftp, snmp) been stopped?		
14.	Has a vulnerability scan been run on this server, and deficiencies addressed?		
15.	Is encryption (i.e. VPN) required when connecting from an external network?		
16.	Is the server backed up regularly, with restore capabilities tested periodically?		
17.	Are the backup tapes/media stored in a separate, secure physical location?		
18.	Is a procedure in place to securely delete data from the server and all backups?		

APPENDIX 2

DEFINITION OF PERSONAL HEALTH INFORMATION (PHI)

The *Personal Health Information Protection Act,* 2004 (PHIPA) defines personal health information (PHI) as information that identifies an individual, e.g. name, and relates to the following. Indicate either yes or no for each identifier, noting whether it will be collected as part of the data collection process.

#	Identifiers	yes	no
1.	Physical and / or mental health, including family health history		
2.	Diagnosis and / or treatment, including the names of care providers		
3.	Service and / or care plans		
4.	Payment and eligibility for healthcare information		
5.	Donations of body parts and substances, including testing or examination		
6.	Health card number		
7.	The identity of a substitute decision maker		

COMMON PHI IDENTIFIERS

The table below is a list of some common identifiers. It is not exhaustive. The key to determining an identifier is the 'small cell' concept. For the purposes of this document, any / all data that can reasonably be expected to identify an individual should be considered personal health information, and as such should be de-identified before disclosure. Indicate in the yes or no column whether the identifiers noted will be collected as part of the data collection process.

#	Identifier	yes	no
1.	Name (first, middle, last and title)		
2.	Location references smaller then province (including postal code, zip code, GIS)		
3.	All elements of birth date, except year (including all indicators of age)		
4.	Dates of treatment in cases where treatment is especially unique or rare		
5.	Telephone number		
6.	Fax number		
7.	Email address		
8.	Social insurance number (SIN)		
9.	Medical record number (MRN)		
10.	Health plan beneficiary number (OHIP number)		
11.	Any / all account numbers		
12.	Certificate or license numbers		
13.	Vehicle identifiers (including license plate)		
14.	Device identifiers (including serial number)		
15.	URL (Uniform Resource Locator – i.e. worldwide web address)		
16.	IP address (internet protocol address)		
17.	Biometric identifiers (use of measurable biological characteristics such as voice, fingerprints, or iris patterns to identify a person to an electronic system)		
18.	Photograph (full face), and any comparable images		
19.	Any other unique identifying characteristic and / or code		

FACTORS TO CONSIDER BEFORE REMOVING IDENTIFIABLE PERSONAL HEALTH INFORMATION (PHI) FROM A HIC

The following factors need to be considered before removing identifiable personal health information from a HIC. Indicate in the yes or no column whether the following items for consideration have been investigated and acted upon.

#	Items for Consideration	yes	no
1.	Have you reviewed your HIC's Storage, Transport and Destruction of Confidential Information policy?		
2.	Will it be necessary for you to remove PHI from a secure HIC environment?		
3.	Have you considered less risky alternatives, such as remote access to PHI stored on secure network storage?		
4.	Have you reviewed your HIC's Remote Access Policy?		
5.	If you must remove PHI from the secure HIC environment, will you keep the number of records, and the number of fields within those records, to the minimum necessary?		
6.	If possible, will you de-identify the PHI to render it anonymous?		
7.	If it is not possible to de-identify the PHI, will you encrypt it?		
8.	Will you protect or have you protected your mobile storage device and / or any files containing PHI with strong passwords?		
9.	If your mobile device is lost or stolen, will you be able to identify all of the PHI stored on it?		
10.	If your mobile device is lost or stolen, do you have the contact information available for your immediate supervisor and the HIC's Privacy Office for immediate notification?		