



Regional Health

POLICIES PROCEDURES STANDARDS GUIDELINES

| | | | |
|------------------------------------|--|-------------------------------|---|
| TITLE: | Privacy of Personal Health Information | NUMBER: | HIS-08 |
| CATEGORY: | Corporate Services & Operations | PAGE: | 1 of 13 |
| DEPARTMENT SERVICE/PROGRAM: | Health Records | POLICY | <input type="checkbox"/> PROCEDURE <input checked="" type="checkbox"/> |
| | | GUIDELINE | <input type="checkbox"/> STANDARD <input type="checkbox"/> |
| INTERNAL DISTRIBUTION: | Organization Wide | EXTERNAL DISTRIBUTION: | |
| APPROVED: | Senior V-P Corporate Services & Operations | APPROVAL DATE: | April 5, 2005 |
| | | REVIEWED: | January 16, 2006 |
| | | REVISED: | |

Thunder Bay Regional Health Sciences Centre (TBRHSC) will respect patients' right to privacy by protecting personal health information in accordance with the Privacy - Personal Health Information Policy, HIS-06, and applicable legislation including the Personal Health Information Protection Act, Public Hospitals Act, Mental Health Act, and others as appropriate.

The purpose of this procedure is to provide staff with an overview of privacy issues related to patient care. This document is not all inclusive of situations that may arise. If further information or clarification is required contact the Manager of Health Records & Admitting who is the designated Privacy Officer. Privacy inquiries from staff, patients, family, etc. should be directed to the Manager of Health Records & Admitting, via e-mail, privacy@tbh.net or phone 684-6056.

The privacy legislation stipulates that all individuals and organizations that have access to or are responsible for patients' personal health information must protect it. Individuals not complying with privacy legislation, policies, and procedures will face disciplinary action up to and including termination of employment or affiliation.

All TBRHSC staff, privileged staff, volunteers, and students have a duty to report any privacy breaches they become aware of. The organization must notify the patient of any breaches that have occurred with their personal health information. Breaches include the sending of reports, fax or mail, to the incorrect recipient.

A privacy breach happens when personal health information is to be accessed, disclosed, used, collected, or disposed of in a way that does not comply with the Personal Health Information Protection Act. Hospital staff, privileged staff, volunteers, and students may be fined \$50,000 whether or not the hospital itself is prosecuted or convicted. A breach of privacy may entitle affected individuals to sue for damages for up to \$10,000.

The collection of accurate information is an important aspect of creating personal health information. It is imperative that the current family physician is verified and that selecting the correct provider in the hospital wide system to ensure incorrect information does not result in a breach of privacy.

Personal Health Information includes personal, demographic, and medical information on all types of format, e.g. electronic, paper.

| | |
|--|-------------------------------------|
| DEFINITIONS | 3 |
| BREACH | 3 |
| CHILDREN’S CONSENT | 3 |
| CIRCLE OF CARE | 3 |
| DE-IDENTIFY | 3 |
| EXPRESS CONSENT | 4 |
| HEALTH INFORMATION CUSTODIAN | 4 |
| IDENTIFYING INFORMATION | 4 |
| IMPLIED CONSENT | 4 |
| INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO | 4 |
| NEED TO KNOW | 4 |
| PERSONAL HEALTH INFORMATION | 4 |
| I. ACCESS TO OR USE OF PERSONAL HEALTH INFORMATION | 4 |
| • <i>Direct patient care</i> | 4 |
| • <i>Education</i> | 4 |
| • <i>Other uses</i> | 5 |
| • <i>Patient’s personal use</i> | 5 |
| • <i>Performance of one’s duties</i> | 5 |
| • <i>Quality Management</i> | 5 |
| • <i>Law</i> | 5 |
| • <i>Research</i> | 5 |
| • <i>Staff accessing their own information</i> | 5 |
| II. DISCLOSURE OR RELEASE OF PERSONAL HEALTH INFORMATION | 5 |
| DISCLOSURE TO A PROVIDER WITHIN THE ‘CIRCLE OF CARE’ | 5 |
| DISCLOSURE TO A PROVIDER OUTSIDE OF THE ‘CIRCLE OF CARE’ WHO IS DIRECTLY INVOLVED IN THE DELIVERY OF CARE AND SERVICES FOR THE THERAPEUTIC AND DIAGNOSTIC BENEFIT OF THE PATIENT | 6 |
| PATIENT’S ACCESS TO INFORMATION | 6 |
| INPATIENT | 6 |
| PATIENTS NOT IN HOSPITAL | 7 |
| VALID AUTHORIZATION | 7 |
| FOUNDATION / DONATION WITHDRAWAL | 8 |
| CARE OR CUSTODY | 8 |
| DECEASED INDIVIDUAL | 8 |
| EDUCATION | 8 |
| FAMILY MEMBERS OR FRIENDS | 8 |
| OTHER PARTIES | 9 |
| PATIENT IS INCAPABLE | 9 |
| POLICE/LAW ENFORCEMENT | 9 |
| RESEARCH | 9 |
| RISK OF HARM | 9 |
| VISITOR INQUIRIES OF PATIENT LOCATION AND STATUS | 9 |
| REMOVAL OF RECORDS | 9 |
| III. IDENTIFICATION | 9 |
| IV. ELECTRONIC TRANSMISSION OF PERSONAL HEALTH INFORMATION | 10 |
| PROCEDURE | 10 |
| 1. <i>Faxing Personal Health Information</i> | 10 |
| 2. <i>Internet/E-mail</i> | 10 |
| SECURITY OF PAPER/HARD COPY INFORMATION | 10 |
| SECURITY OF ELECTRONIC PATIENT INFORMATION | 10 |
| i. <i>Administrative Procedures</i> | 10 |
| ii. <i>Physical Safeguards</i> | 10 |
| iii. <i>Technical Security</i> | 10 |
| BREACH OF PRIVACY AND CONFIDENTIALITY INVESTIGATION PROCESS | ERROR! BOOKMARK NOT DEFINED. |
| CONSENT REQUIREMENTS | 12 |
| REFERENCES | 13 |

Definitions

Breach

A privacy breach occurs when personal health information is disclosed, shared, collected, used, or disposed of in a way that does not comply with the Personal Health Information Protection Act. Types of breaches are:

- unauthorized access of personal health information by staff, e.g. comment on co-worker who is receiving treatment at TBRHSC to other co-workers or anyone outside the organization or telling family members or friends who you saw at TBRHSC
- unauthorized disclosure through loss, theft, or mistake
- disposal of personal health information in a method that is not secure
- disposal of a record of personal information in an attempt to evade an access request

Breaches include the sending of reports, fax or mail, to the incorrect recipient.

Children's Consent

Children of any age are presumed to have the capacity to consent to the collection, use and disclosure of their personal health information. Do not presume capacity if it is not reasonable to do so in the circumstances.

For children under 16, a parent or other lawful guardian may consent to the collection, use or disclosure of personal health information even if the child has capacity, unless the information relates to:

- treatment within the meaning of the Health Care Consent Act, 1996 about which the child has made their own decision, or
- counseling in which the child has participated on their own under the Child and Family Services Act.

When you need consent for the collection, use or disclosure of information about a child less than 16, you may either obtain it from that child, if capable, or the parent or other lawful guardian (but not the access parent, unless such a parent has been lawfully authorized in place of the custodial parent to make information decisions). If there is a conflict between the child and the parent, the capable child's decision prevails with respect to the consent.¹

Circle of Care includes individuals who are directly involved in the delivery of care and services for the therapeutic and diagnostic benefit of the patient. The individuals may include a person who is one of the following or operates one of the following:

- Health care practitioners and groups of health care practitioners
- Public and private hospitals
- Pharmacies
- Laboratories
- Ambulance services
- Community care access centres
- Community service providers (defined in the Long Term Care Act)
- Psychiatric facilities
- Independent health facilities
- Homes for the aged, rest homes, nursing homes, care homes and homes for special care, and
- Community health or mental health centres, programs and services whose primary purposes are providing health care²

De-identify in relation to the personal health information of an individual, means to remove any information that identifies the individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify the individual, and "de-identification" has a corresponding meaning.³ Name removal may not be sufficient to de-identify personal health information in cases with unique factors.

¹ Definition adapted from OHA Privacy Toolkit, Sept 2004

² Definition adapted from OHA Privacy Toolkit, Sept 2004

³ Definition adapted from the Personal Health Information Protection Act, 2004

Express consent refers to consent obtained directly from the patient or substitute decision-maker through an oral or written request specific to the situation

Health information custodian A person or organization who has custody or control of personal health information as a result of or in connection with performing the person's or organization's powers or duties, e.g. hospital, nursing home, pharmacy, ambulance service, medical officer of health, or board of health, Ministry of Health, etc.

Identifying information means information that identifies an individual or for which it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual. Name removal may not be sufficient to de-identify personal health information.

Implied consent refers to consent obtained through the action of the patient. For example, by coming to the hospital and answering questions, the patient is implying that we may use the information for the purposes that we have communicated to the patient. Implied consent is used for the purposes communicated to the patient through privacy notices made available throughout the organization.

Information and Privacy Commissioner of Ontario oversees compliance with the Act. Patients have the right to file a complaint with the Commissioner if they are not satisfied with our response to their access, correction, or breach investigation process.

Need to know means the principle that a staff member should have access only to the personal health information needed to perform a particular function.

Personal health information means identifying information about an individual in oral or recorded, paper and electronic form, if the information:

- relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family
- 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
- is a plan of service within the meaning of the *Long-Term Care Act, 1994* for the individual
- relates to payments or eligibility for health care in respect of the individual
- 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
- is the individual's health number; or
- identifies an individual's substitute decision maker

I. **Access To or Use of Personal Health Information**

1. **Access to health information** - is based on the "need to know" principle to provide current and direct patient care or to perform one's duties. Personal health information may be used only under the following conditions:

- **Direct patient care** – the health care provider may access health information when they are involved in the direct and current care of the patient. Access to health information is limited to that information which is required to fulfill the purpose of care. There must be a plan that the patient is being transferred to a staff's unit before they access the patient's information. It is not acceptable to access patient's information you treated in the past because of interest in the outcome of care. See Disclosure section of this procedure.
- **Education** – Personal health information may be used in education rounds for teaching purposes providing no identifiable information is disclosed. Identifiable patient information will be used only where necessary for internal clinical education purposes. Express consent from affected patients is required if you disclose personal health information to health care practitioners or students who are not staff, privileged staff, or students of TBRHSC. For example if you disclose personal health information at grand rounds at TBRHSC, but outside guests are at the rounds, express consent must be obtained.

- Other uses – When used for purposes other than those stated above, personal health information may be accessed only by persons authorized by the patient through express consent.
- Patient's personal use – Patients' generally have a right to access their personal health information through the organization's Release or Disclosure of Information section of this procedure.
- Performance of one's duties – Personal health information may be accessed by staff to perform their job duties only after there is a definite plan that the patient will be cared for in their area. For example, if a patient is in the Emergency Department and Admitting has notified a unit the patient will be transferred to their unit, only after notification from Admitting would it be acceptable for staff to access the patient's record to plan for their arrival. It is not acceptable for staff to peruse patients' records in the event they may be admitted to their unit.
- Quality Management – Personal health information may be used to ensure that quality care and services are provided to patients.
- Law – Personal health information may be accessed and/or released as required by law.
- Research – Personal Health Information may be used for this purpose once the study is approved by the Research Ethics Team, a research plan is in place and all administrative approvals have been received. All patient identification must be removed prior to presentation or publication of results. See policy Admin-13.
- Staff accessing their own information - Accessing patient information is on a need to know basis to perform responsibilities as an employee. Staff accessing their own record is in the role of a patient. Staff are to follow the same process as patients; access is through the Health Records Department upon completion of the form, Patient's Request for Access to Personal Health Information, form number CS-346. Staff must provide patient's authorization to review a family member or friend's information. The same process applies for electronic and paper information. The request is to be made in writing or complete the hospital form, "Patient Request for Access to Health Information", form number CS-346, and present it to the Health Records Department.

2. **Disciplinary action**

The privacy legislation states that all individuals and organizations that have access to or are responsible for patient's personal health information must protect it. Individuals not complying with privacy legislation, policies, and procedures will face disciplinary action up to and including termination of employment or affiliation.

The Personal Health Information Protection Act stipulates it is an offence to access, disclose, or collect personal health information in breach of the law. Hospital staff, privileged staff, volunteers, and students may be fined \$50,000 whether or not the hospital itself is prosecuted or convicted. A breach of privacy may entitle affected individuals to sue for damages for up to \$10,000. See Breach of Privacy and Confidentiality Investigation Process page 11.

II. **Disclosure or Release of Personal Health Information**

Disclosure to a provider within the 'circle of care'

Personal health information can be disclosed to providers who are directly involved in the delivery of care and services for the therapeutic and diagnostic benefit of the patient (circle of care) without the express consent of the patient unless the patient has expressly revoked consent. Exceptions to this are:

- When the patient introduces a new provider into the circle of care, express consent from the patient is required before disclosing any personal health information to this new provider.

- When a provider within the circle of care introduces a new provider to the circle of care, implied consent can be used based on the referral.
Providers may not necessarily be employees of TBRHSC, i.e. CCAC staff, etc.

Family physicians are considered part of the circle of care if the patient identifies the physician as the family physician at the time of admission or visit or otherwise provides the information. Implied consent can continue to be used when providers require access to personal health information about a visit where they were part of the circle of care even if the information is required after the visit is completed. It is imperative that staff verifies with each patient the current family physician. Failure to do so may result in a breach of privacy.

Disclosure to a provider outside of the 'circle of care' who is directly involved in the delivery of care and services for the therapeutic and diagnostic benefit of the patient

- (a) Patient or substitute decision-maker consent is required to provide personal health information to a health information custodian outside the 'circle of care'.

Patient's access to information

When patients ask to view and/or receive copies of their own Personal Health Information, they will be asked to complete the Patient's Request for Access to Personal Health Information Form, number CS-346 or to submit the request, identifying all required information in the form of a letter.

Generally, a patient has a right of access to a record of personal health information about the individual that is in our custody with the following exceptions:

- (a) the information is subject to a legal privilege that restricts disclosure to the individual
- (b) legislation or a court order prohibits disclosure to the individual of the record or the information in the record in the circumstances
- (c) the information was collected or created primarily in anticipation of or use in a proceeding
- (d) the information was collected or created in the course of an inspection, investigation or similar procedure authorized by law
- (e) granting the access could reasonably be expected to result in a risk of serious harm to the treatment or recovery of the individual or another person. The clinical or physician leader may be contacted and advised of the request for disclosure of personal health information
- (f) granting access could lead to the identification of a person who was required by law to provide information in the record
- (g) granting access could lead to the identification of a person who provided information in the record in confidence and it is considered appropriate to keep the name of the person confidential

If none of the above conditions apply, the patient will be given an appointment to view or obtain copies of the information. If any of these conditions apply, inform the patient in writing and notify the Manager of Health Records & Admitting.

Inpatient

All third party, non-medical requesters, e.g., insurance company, should be referred to the Correspondence Technician, Health Records Department or appropriate department if information is stored elsewhere. Consents for non-medical requests must be in writing.

When a patient presently being treated at TBRHSC requests access to their information, the Clinical Manager will deal with the request, applying the following steps:

- Notify the attending physician
- Set an appointment time that does not interfere with the care being given
- Allow the patient access to their medical record only in the presence of a member of the medical or clinical staff to ensure the integrity of the record is maintained
- Explanation of terms and abbreviations in the record will be provided by the medical or clinical staff in attendance

Assistance is available by contacting the Health Records Manager, Co-ordinator, or Correspondence Technician.

Should the patient disagree with information in the record, they may request a change to the health record in writing through the Health Records Department. The patient is not permitted to alter, deface, or remove any part of the personal health information. The Request for Correction to Personal Health Information Form, number CS-349, will be completed by the patient.

If the patient requests copies of their record, a charge is applicable if the copies are for non-medical use. Contact the Health Records Department for fees and billing process.

Patients Not In Hospital

Requests for personal health information will be processed by Health Records Staff, with the exception of requests for reports that are maintained in Mental Health, Diagnostic Imaging, Social Work, Rehabilitation, Cardio-Respiratory, Psychology, and Utilization.

Valid Authorization

It is a requirement that the original signature of the person whose information is to be released, or that of the person's legally authorized representative, is obtained. Reproductions of original signatures will not be accepted.

Requests for release of information for individuals under the age of 16 will be accepted from parent(s)/legal guardian(s) unless we are aware that the parent(s)/legal guardian(s) and patients wishes are not the same and that the patient is capable of consenting. In this case, a request must be made by the patient. If there is reason to doubt the custodial relationship of the requestor, proof of custody will be required.

If the patient is not capable of consenting to the collection, use, or disclosure of personal health information obtain consent (ranked in order as listed) from the patient's:

- guardian
- attorney for personal care or attorney for property (if the attorney has the authority to make such decisions)
- representative (appointed by the Consent and Capacity Board under the Health Care Consent Act, if the representative has the authority to give the consent)
- spouse or partner
- child, custodial parent, Children's Aid Society, or other person legally entitled to give or withhold consent in place of a parent (Note: where this is the situation, the child's parent cannot consent on behalf of the child)
- parent with access rights
- brother or sister
- other relative, related by blood, marriage or adoption⁴

Other Facility Personal Health Information Required

In the event that patient information is required from another facility and the patient is unable to give consent, the request should be forwarded to the Health Records Department. If the Health Records Department is closed, the Administrative Co-ordinator should be contacted.

Authorized staff, i.e. Health Records, Mental Health Clerk-Typists, etc. may release personal health information with appropriate consent as outlined below:

- a) All requests for personal health information after patient discharge or attendance should be made in writing and contain the following:
 - i. Name and address of the recipient of the information
 - ii. Purpose or need for information
 - iii. Full name, address, and date of birth of the person whose information is being requested
 - iv. Specific definition of the type and extent of the information required
 - v. Relevant treatment dates, and

⁴ Definition adapted from OHA Privacy Toolkit, September 2004

- vi. Name of person authorizing the personal health information
 - vii. A complete, witnessed, Consent to Disclose Personal Health Information Form, number CS-348 or letter from the patient containing all required information
- b) The Form or Letter is filed with the patient's personal health information.

Foundation / donation withdrawal

A patient or substitute decision-maker may withdraw their consent to be contacted by the Foundation at any time by notifying the Manager of Health Records & Admitting, phone 684-6056. A patient's withdrawal has no effect on information collected, used, or disclosed before the patient withdrew their consent, but has effect from the time it is received. Patients that have given implied consent will have only their names and mailing addresses made available to the Foundation.

Care or custody

Personal Health Information may be disclosed about an individual to the head of a penal or other custodial institution in which the individual is being lawfully detained or to the officer in charge of a psychiatric facility within the meaning of the Mental Health Act in which the individual is being lawfully detained for the following purposes:

- arrangements for the provision of health care to the individual; or
- the placement of the individual into custody, detention, release, conditional release, discharge or conditional discharge under Part IV of the Child and Family Services Act, the Mental Health Act, the Ministry of Correctional Services Act, the Corrections and Conditional Release Act (Canada), Part XX.1 of the Criminal Code (Canada), the Prisons and Reformatories Act (Canada) or the Youth Criminal Justice Act (Canada).

Deceased Individual

Personal health information about an individual who is deceased can be disclosed for the following purposes:

- (a) identifying the individual
- (b) informing any person whom it is reasonable to inform in the circumstances (e.g. spouse, children, close friend) of,
 - (i) the fact that the individual is deceased or reasonably suspected to be deceased, and
 - (ii) the circumstances of death, where appropriate; or
- (c) to the spouse, partner, sibling, or child of the individual if the recipients of the information reasonably require the information to make decisions about their own health care or their children's health care.

Any additional information should be released only to the estate trustee. Refer requests to Health Records Department, Correspondence Technician or Mental Health Clerk-typist if request pertains to Mental Health Program.

Education

De-identify information about a patient when you disclose patient case details to health care practitioners for formal educational programs where possible.

Express consent from affected patients is required if you disclose personal health information to health care practitioners or students who are not staff, privileged staff, or students of TBRHSC. For example if you disclose personal health information at grand rounds at TBRHSC, but outside guests are at the rounds, express consent must be obtained.

Family members or Friends

Personal Health Information about a patient can only be disclosed with the patient's or substitute decision-maker's consent. Follow these steps to comply with the request:

- Verify that the patient or substitute decision-maker has consented to the disclosure of the personal health information to the patient's family members or friends
- Understand the purpose for which the personal health information is being requested
- Disclose only personal health information for which you have consent to disclose and that serves the purpose for which the disclosure is requested
- Confirm the family member's or friend's identity

Document the date of the request and the disclosure of the personal health information in the patient's record

Other Parties

Personal Health Information may be released to another party with patient or substitute decision maker's consent as required by law and outlined in this section. The request must follow the requirements in Section II of this policy.

Patient is incapable

Personal health information can be disclosed for the purpose of identifying a substitute decision-maker if the individual is injured, incapable, or ill and unable to give consent personally.

Personal health information can be shared with the substitute decision-maker as needed to make decisions about the patient's care while a patient is at TBRHSC.

Police/Law Enforcement

Express patient consent is required when the request for personal information is not covered by a warrant.

Patient consent is not required in the following circumstances:

- (a) Where the request is being made on behalf of the Coroner for an investigation or death inquest and evidence of this request is provided (a written request).
 - (b) When the law enforcement officers have a warrant for personal health information
 - (c) Where a health care provider is the victim of a crime (as required by the Criminal Code of Canada).
- Police making inquiries as to the location of patients should be directed to Administration or the Administrative Co-ordinator during off hours.

Research

Personal Health Information may be disclosed for the purposes of research if the researcher has been approved by the Research & Ethics Team, Policy No. Admin-13.

Risk of harm

Personal Health Information may be disclosed about an individual if the privileged staff, manager, or Administrative Co-ordinator believes disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm to a person or group of persons.

Visitor inquiries of patient location and status

The following Personal Health Information may be disclosed relating to an individual who is a patient at TBRHSC unless the patient has objected to this disclosure:

1. The fact that the individual is a patient in the facility
2. The location of the individual in the facility

Contact Switchboard if the patient expressly requests that visitors not be notified they are in the facility.

Police making inquiries as to the location of patients should be directed to Administration or the Administrative Co-ordinator during off hours.

Media inquiries should be directed to your Manager/Director.

Removal of records

Personal Health Information may not be removed from TBRHSC unless it is in accordance with a subpoena, warrant, court order, other process issued in Ontario, or in accordance with statutory authority.

III. Identification

It is imperative that identification be shown by any person receiving patient information, e.g., police, former patient, etc. to verify information is only being released to appropriate individuals. Police officers' name and badge number should be recorded on the documentation provided.

IV. Electronic Transmission of Personal Health Information

If a fax is sent to an incorrect recipient, contact the Manager of Health Records & Admitting.

Procedure

1. Faxing Personal Health Information

- Use automatic dialling features for frequently dialled numbers to eliminate the possibility of incorrect dialling
- Visually check on the fax machine to assure the correct number was dialled, if not using automatic dialling features
- Discrimination should be used to determine the appropriateness of using fax as a means of transmitting personal health information
- When consent is required, a faxed copy will be acceptable with the understanding that the original consent will be forwarded by mail as soon as possible
- Sender of information shall be responsible for seeking confirmation of appropriate transmission
- Ensure a cover page accompanies the faxed personal health information; cover page should include the sender's name, department, phone number, fax number, the recipient's name, department, and number of pages being transmitted
- Fax machine should be located in a secure area
- A record of the transaction consisting of what information was transmitted, who it was sent to, the date of transmission, and the name of the sender must be kept on file

2. Internet/E-mail

External e-mail

Patient names or patient information is not to be sent using e-mail

Internal e-mail

Patient names or patient information is permissible within TBRHSC and St. Joseph's Care Group

Security of paper/hard copy information

Personal health information must be stored in a secure area and not left unattended in areas accessible to unauthorized individuals. It is imperative that personal health information be secured in areas that are not staffed 24/7.

Security of electronic patient information

Security applies to the spectrum of physical, technical, and administrative safeguards put into place to protect the integrity, availability, and confidentiality of electronic patient information.

i. Administrative Procedures

- All sources of patient information are identified
- Documented procedures for securing the data are in place
- Passwords are required to access information
- Access is controlled by minimum necessary provisions on a "need to know" basis
- Confidentiality agreements are signed by users of the systems
- Application use is controlled by password logon and timeout logoffs
- Audit trails of electronic personal health information are available, and audits are performed
- Training is provided in applications prior to granting access
- Downtime procedures are in place

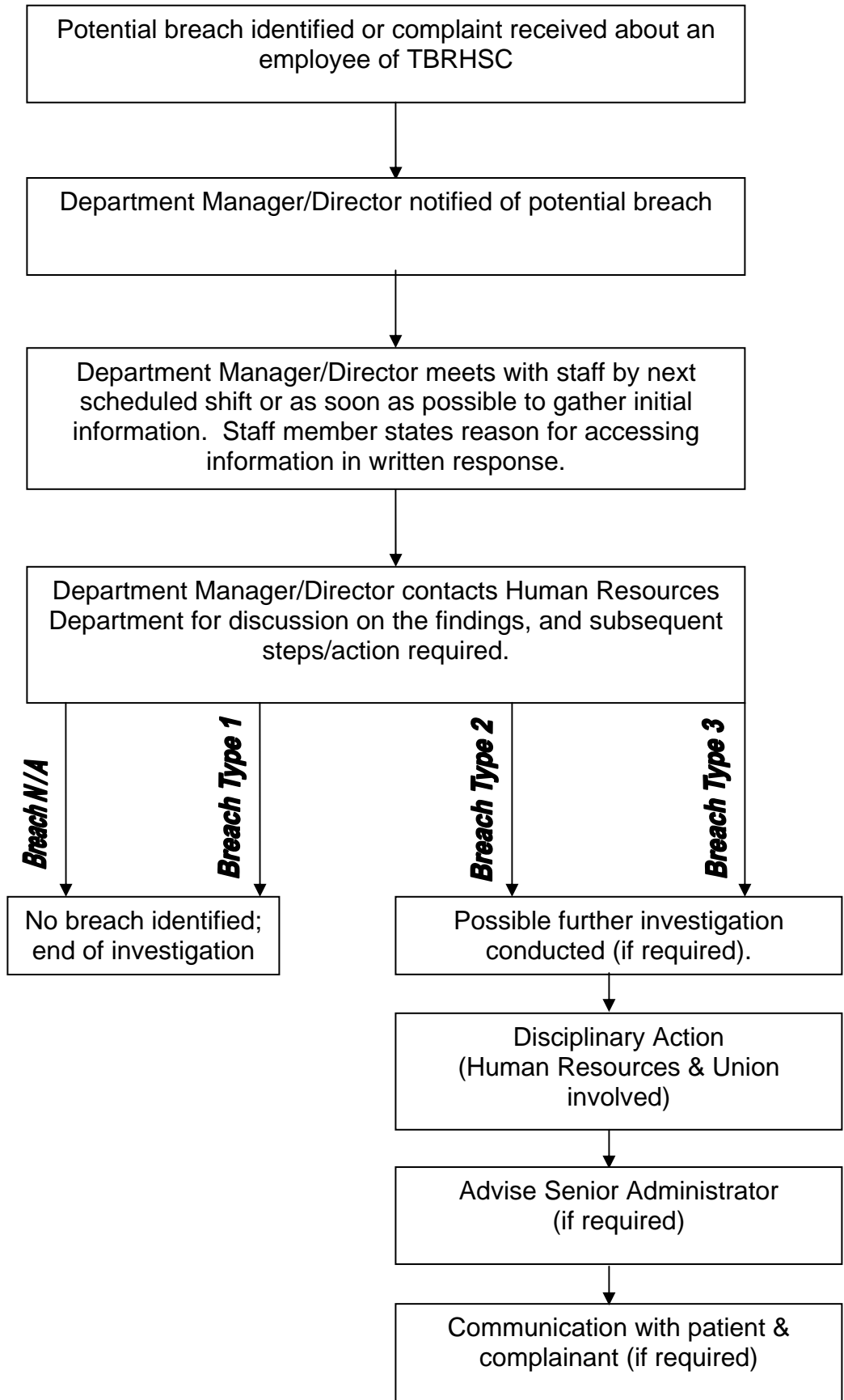
ii. Physical Safeguards

- Locked/badge access to computer room and to server rooms
- Off-site storage of tapes/disks in a fire-rated enclosure
- Computer room access audits are reviewed when required

iii. Technical Security

- Data back ups will be performed daily
- Regular power, emergency diesel power, and UPS (Uninterruptible Power Supply) are available
- RAID technology is used provide a second copy for redundancy
- Enterprise Backup System in place

Breach of Privacy and Confidentiality Investigation Process



Consent Requirements

| Person/Institution requesting Patient's Record | Patient Consent Required |
|--|--|
| College under the RHPA | No |
| College of Nurses | No |
| College of Physicians & Surgeons of Ontario | No |
| Community Services, e.g., VON., Thunder Bay Orthopaedic, Home Care | No, however patient may withdraw their implied consent |
| Coroner | No |
| Criminal Injuries Board | Yes |
| Employer | Yes |
| Family & Children's Services If CAS is the crown ward, have apprehended, have temporary care, or our staff initiated investigation All other circumstances | No Yes |
| Hospitals, other direct transfer | No |
| Insurance Company | Yes |
| Lawyer | Yes |
| North of Superior Programs | Yes |
| Person on behalf of patient, e.g. relative | Yes |
| Physician, dentist, midwife attending Physician, dentist, midwife, not attending | No Yes |
| Police no warrant order, warrant or other process issued by Court in Ontario, subpoena | Yes No No |
| Probation and Parole Services | Yes |
| Substitute Decision Maker | No |
| Workers Compensation | No |
| Thunder Bay District Health Unit - Genetic Counselling - A reportable or communicable disease | Yes No |

REFERENCES

Bill 31: An Act to enact and amend various Acts with respect to the protection of health information. Royal Assent, May 20, 2004, 38th Parliament, 1st Session, 2003-2004. Toronto: Legislative Assembly of Ontario, 2004. Available: http://www.ontla.on.ca/documents/Bills/38_Parliament/Session1/b031ra.pdf . [October 22, 2004]

“Personal Health Information Protection Act” Toronto: Legislative Assembly of Ontario, 2004. Available: http://www.e-laws.gov.on.ca/DBLaws/Statutes/English/04p03_e.htm [October 22, 2004]

Ontario Hospital Association, Ontario Hospital eHealth Council, Ontario Medical Association, Office of the Information and Privacy Commissioner. 2004. Hospital Privacy Toolkit: Guide to the Ontario Personal Health Information Protection Act. (Publication # 314). Ontario: Queen’s Printer for Ontario.

Ontario Hospital Association. 2003. Guidelines to Managing Privacy, Data Protection and Security for Ontario Hospitals. Ontario: