


<b>Title:</b> Research Data Stewardship & Security of Health Information	<input checked="" type="checkbox"/> Policy	<input type="checkbox"/> Procedure	<input type="checkbox"/> SOP
<b>Category:</b> General <b>Dept/Prog/Service:</b> Research: Clinical Research	<b>Distribution:</b> Organization Wide		
<b>Approved:</b> Vice President, Research <b>Signature:</b> 	<b>Approval Date:</b>	Nov. 1, 2016	
	<b>Reviewed/Revised Date:</b>		
	<b>Next Review Date:</b>	Nov. 1, 2019	

**CROSS REFERENCES:** (HIS-08) Privacy of Personal Health Information Policy; (CR-01) Investigator Responsibilities for the Conduct of Research Involving Humans; (RA-01) Research Integrity; (ADMIN-04) Record Retention; (CR-06) Project Registration and Authorization; (IS-USE-013-N) Appropriate Use of Technology & Security; (IS-SEC-022-N) Data Disposal - Electronic

### 1. PURPOSE

Define the obligations and responsibilities of the Researcher in protecting and securing personal health information disclosed to them for the purpose of research.

### 2. POLICY STATEMENT

The Researcher is assigned as the steward for all research data generated from research in which he/she is engaged as Principal Investigator. This includes operational responsibilities and the responsible management of research data - see Policy ADMIN - 31 – Research Integrity, CR- 01 – Investigator Responsibilities for the Conduct of Research Involving Humans, and ADMIN-04 – Record Retention.

Researchers must protect data used for research purposes and maintain its privacy. In a modern environment with multiple methods of data storage and transmission, the obligation to protect data requires increased vigilance. See Privacy of Personal Health Information Policy HIS-08 – and IS-USE-013-N – Appropriate Use of Technology & Security. All of these considerations must be included in the approved research protocol.

As the steward of the research data, the Researcher will ensure that data is maintained for the required retention period in an available format. The Researcher will ensure that any secondary uses of the data are consistent with any funding agreements, contractual obligations, third-party agreements, approved protocols, and legal and regulatory requirements, including consent provisions where required.

### 3. SCOPE

Everyone with access to Research data working at or with Thunder Bay Regional Health Sciences Centre (The Hospital) or Thunder Bay Regional Health Research Institute (The Institute) is responsible for the protection of research data including personal health information (PHI).

### 4. PROCEDURE

#### 5.1 Collection of Data from Humans & Personal Health Information (PHI)

Collection and use of data for research requires appropriate consent, approval of the protocol through research ethics, and authorization of the research project by the Vice President Research – see CR-07 – Project Registration and Authorization. This includes data for future research purposes, as well as data collected in conjunction with biological specimens. (Note: collection of data for quality assurance purposes should follow existing

This material has been prepared solely for use at Thunder Bay Regional Health Sciences Centre (TBRHSC). TBRHSC accepts no responsibility for use of this material by any person or organization not associated with TBRHSC. No part of this document may be reproduced in any form for publication without permission of TBRHSC. A printed copy of this document may not reflect the current electronic version on the TBRHSC Intranet.

hospital protection of personal health information (PHI) as per Privacy policy HIS-08 and does not require research Authorization.)

Researchers must maintain data in a secure, de-identified, and encrypted manner consistent with appropriate policies and legislation. This information must be provided in the approved protocol for the research project. In addition to research Authorization, approval from the Sr. Director of Informatics via the "Information Sharing Agreement" is also required – contact Informatics.

## 5.2 Research Data Retention

Research data must be retained by the Researcher for the required retention period. Researchers are responsible for storage/retention of research data for a minimum of 10 years after the research project has ended or according to the following list, whichever is longer. A research project or activity should be regarded as having ended after (a) final reporting to the research sponsor, (b) final financial closeout of a sponsored research award, or (c) publication of research results, whichever is later.

Records must be maintained for the maximum duration required by:

- Admin-04 Record Retention;
- specific funding and regulatory agencies;
- a publishing journal;
- the terms of a research agreement;
- to protect intellectual property rights;
- TBRHSC in the event of a research misconduct allegation.

Data is to be stored in a manner that is retrievable during the retention period.

Following the minimum retention period, retention of the research data will be reevaluated by the Vice President of Research and Sr. Director of Informatics, and, if appropriate, the data will be destroyed in a manner appropriate to the type of data and the medium in which it is stored. (See Policy IS-SEC-022-N – Data Disposal – Electronic).

## 5.3 Responsibilities

### The Researcher

- Ensures appropriate preparation and transfer of data into existing public repositories as required by funders and regulators. Where applicable, should request funding from the granting agency to cover the cost of preparation and transfer of data.
- Ensures retention and storage requirements are met for research data.
- Facilitates access to data for auditing.
- Ensures use of hospital-approved encrypted devices such as USB keys, hard drives, servers, and laptops for storage of data.
- Ensures PHI is stored securely.
- Ensures appropriate handover of responsibilities upon leaving the institution.
- Ensures that all actions of members of their research teams in relation to data conform to this policy.
- Where PHI or other confidential information is handled:
  - a. Requires his/her research teams are trained in data management.
  - b. Ensures appropriate consent and agreements for sharing/transferring of data are in place.
  - c. Works with de-identified data at all times, except when identifiable data is absolutely required – as per the approved research protocol.

---

Also see - Policy ADMIN-31 – Research Integrity, CR-01 – Investigator Responsibilities for the Conduct of Research Involving Humans, and ADMIN-04 – Record Retention

**The Hospital**

- Facilitates agreements and the sharing and protecting of data, where applicable.
- Administers the rights of data ownership – if governed by a Research Agreement.
- Performs audits of research data against applicable standards.
- Assesses equipment that will retain and/or store PHI to ensure adequate security controls are in place.

**6. REFERENCES**

*Policy Number 40.50.004* – University Health Network Policy on Data Ownership, Stewardship & Security of Health Information