DALHOUSIE UNIVERSITY Health Data Nova Scotia **Data Retention and Destruction Policy**	**Author:** S.Kennedy	**Review Date:** 01.01.2018
	Approved by and date: S.Carrigan / 05.04.2017	**Effective Date**: 05.04.2017
	Version Number: v1.0	***Page 1 of 3***

1. BACKGROUND & PURPOSE

1.1 General privacy principles and obligations under the *Personal Health Information Act (PHIA)* require that personal health information (PHI) be retained only as long as necessary for the fulfillment of the research or health service assessment projects purpose. *PHIA* requires that all custodians and their agents have a written retention schedule for PHI that includes:

(a) All legitimate purposes for retaining the information; and

(b) The retention period and destruction schedules associated with each purpose.

2. APPLICATION

2.1 This policy applies to the Health Data Nova Scotia (HDNS) Manager, the System Administrator, and the Finance and Administrative Officer.

3. DEFINITIONS

3.1 *Data Access Committee (DAC)*: The Committee tasked with reviewing requests to conduct secondary data analysis for research or health service assessment purposes using the administrative databases held by HDNS for privacy, security, and confidentiality concerns.

3.2 *Health Service Assessment*: activity to assess, investigate or evaluate the provision of healthcare services.

3.3 *Personal Health Information (PHI):* Identifying information about an individual, whether living or deceased, and in both recorded and unrecorded forms, if the information:

(i) relates to the physical or mental health of the individual, including information that consists of the health history of the individual's family,

(ii) relates to the application, assessment, eligibility and provision of health care to the individual, including the identification of a person as a provider of health care to the individual,

(iii) relates to payments or eligibility for health care in respect of the individual,
(iv) 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,
(v) is the individual's registration information, including the individual's health-card number, or
(vi) identifies an individual's substitute decision-maker.

3.4 *Research*: A systematic investigation designed to develop or establish principles, facts or generalizable knowledge, or any combination of them, and includes the development, testing and evaluation of research.

3.5 *Research Ethics Board (REB)*: An REB established and operating in conformity with the Tri-Council Policy Statement. A body of researchers, community members, and others with specific expertise (e.g. research ethics, or relevant research disciplines) established by an institution to review the ethical acceptability of all research involving humans conducted within the institution's jurisdiction or under its auspices.

3.6 *Securely destroyed*: Data which are destroyed in such a manner that reconstruction is not reasonably foreseeable.

4. POLICY STATEMENT

4.1 HDNS datasets used for research and health service assessment projects are extracted, linked, and maintained on the HDNS Secure Data Platform for the length of a project as approved by the HDNS Data Access Committee (DAC) and the Research Ethics Board (REB) (if applicable). Datasets are project-specific and can be easily identified for archival, monitoring, restoration, or destruction.

5. PROCEDURES

5.4 *Retention*

5.4.1 Once a project has received HDNS approval for data access, the start date for access is noted in the project file.

5.4.2 Upon project completion, all project-associated data and the programming code will be archived on the HDNS system for the required time. In lieu of an REB-determined period of storage, code and project data will be archived for seven (7) years following project completion. Project completion is identified by the principal investigator or by lack of annual renewal of data access or REB approval.

5.4.3 The original datasets created out of the HDNS data holdings are retained in accordance with project-specific data sharing agreements, contractual agreements for data access, and REB approvals, but are kept in linked formats for no longer than seven (7) years.

5.4.4 Copies of programs, documentation, and other files that do not contain PHI or other personal information will be archived indefinitely.

5.4.5 The HDNS Secure Data Platform is backed up regularly for the protection of HDNS work products and restoration in the case of disaster. These backups are kept indefinitely.

5.5 *Destruction by HDNS*

5.5.1 HDNS will destroy data provided or linked as part of projects as outlined in any data sharing agreements and HDNS guidelines.

5.5.2 Data are considered destroyed on the HDNS Secure Data Platform if they are removed or deleted from the platform. If the data were stored on removable electronic media, then the media will be erased and re-written using a software utility identified by the HDNS System Administrator. Physical destruction (shredding, burning, de-gaussing, etc.) is also suitable. The final removal from the platform of project datasets at the completion of the project will be documented by the System Administrator.

5.6 *Restoration*

5.3.1 Restoration of data from backups or archives will only be done for disaster recovery or if required for specific projects.

5.3.2 Data will only be restored from backup or archive with the approval of the HDNS Manager in accordance with and the DAC.

6. ADMINISTRATIVE STRUCTURE

6.4 *Accountability*

6.4.1 The Finance and Administrative Officer is responsible to track the progress of projects, ensure that yearly renewals are complete, and record the completion date of the project.

6.4.2 The System Administrator is responsible to securely destroy the project datasets at the appropriate time and record the destruction. This is to be reported to the HDNS Manager and Finance and Administrative Officer.

6.5 *Monitoring and Reporting*

6.2.1 The Finance and Administrative Officer monitor the status of the files and reports back to the HDNS Manager and the DAC as required.

7. RELATED POLICIES AND OTHER DOCUMENTS

7.4 *HDNS Policies and Procedures*

7.2 HDNS Forms

- Project Data Retention Schedule

7.3 Other Documents