DALHOUSIE UNIVERSITY Health Data Nova Scotia **Privacy, Confidentiality and Security Training 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 The purpose of this policy is to set out an overview of the content to be included in privacy, confidentiality and security training ("privacy training") provided by Health Data Nova Scotia (HDNS) and the procedures in providing the training.

2. APPLICATION

2.1 This policy applies to all authorized personnel and approved HDNS users.

3. DEFINITIONS

3.1 *Approved Users:* Individuals who have been issued an access account, key code, and/or swipe card following the approval of access to HDNS data holdings according to the relevant procedures. Approved users may include students, trainees, researchers, health service assessment analysts and other users of the HDNS such as government staff and research analysts.

3.2 *Authorized Personnel*: Individuals who have been authorized to access the HDNS system and/or data holdings and include: HDNS staff and contractors (including system administrators/managers, analysts, documentation specialists), and Dalhousie University Information Technology Support staff.

4. POLICY STATEMENT

4.1 To ensure compliance with legislation, privacy principles, and policies and procedures, HDNS Approved Users must be knowledgeable about the following:

- the right to privacy and the duty of confidentiality,
- the rationale and requirements for limiting use, disclosure and retention of data imposed by personal health information (PHI) legislation,
- overview of HDNS and its mission,
- available HDNS data holdings,

- the importance of the level of detail required when requesting access to data sets (e.g. identification of variables, persons who will have access to data, use of data etc.),
- Data access agreements and their terms,
- Data access and use procedures,
- the administrative, technical and physical safeguards used to protect PHI,
- dissemination of research findings,
- relevant HDNS policies and procedures,
- the duties and responsibilities regarding the identification, reporting, containment and participation in the investigation and remediation of privacy breaches,
- the consequences of breaching privacy.

4.2 All authorized personnel and approved users are required to attend privacy and security training prior to accessing HDNS computers and data for the first time.

4.3 As staff, other authorized personnel, and approved users require differing levels of access, the privacy training will be customized according to the role and the type of access to the HDNS system and data.

5. PROCEDURES

5.1 Orientation and Ongoing Training for Personnel

5.1.1 The HDNS Manager or delegate will contact new users by email prior to their start date to inform them of the requirement for privacy training.

5.1.2 All new personnel are required to attend privacy training within the first week of their commencement of work and prior to access to HDNS data.

5.1.3 Personnel are required to complete ongoing privacy training / updates whenever there is a significant change to legislation, policies, or procedures.

5.1.4 A log to track attendance by personnel at ongoing privacy training is kept by the HDNS Finance and Administrative Officer.

5.1.5 If any personnel have not completed the required privacy training or updates, their access to HDNS data will be withheld until they do.

5.2 Approved Users Training

5.2.1 Once a requestor(s) has received written approval from HDNS for access to data, but before the research project starts, all persons who will have access to line-level HDNS data for the purposes of the project, will be informed by HDNS of the date that they must complete privacy training.

5.2.2 All approved users must complete the privacy training prior to accessing HDNS data.

5.2.3 Documentation of the completion of the training will be kept by the HDNS Finance and Administrative Officer.

5.2.4 Whenever there is a significant change to legislation, policies, procedures, the HDNS Manager will provide privacy updates to approved users.

6. ADMINISTRATION

6.1 Accountability

6.1.1 The HDNS Manager is responsible for ensuring the development, revision, provision, and tracking of privacy training to authorized personnel and approved users.

6.1.2 Authorized Personnel and Approved Users are responsible to complete the required training.

6.2 Monitoring, auditing and reporting

6.2.1 A log to track completion of initial and ongoing privacy training will be maintained by the HDNS Finance and Administrative Officer.

6.2.2 The HDNS Manager incorporate any recommendations with respect to privacy training made in privacy impact assessments, privacy audits and the investigation of privacy incidents, breaches or complaints.

7. RELATED POLICIES AND OTHER DOCUMENTS

7.1 HDNS Policies and Procedures

- Policy manual

7.2 HDNS Forms

- Privacy, Confidentiality and Security Training Log

7.3 Other Documents