DALHOUSIE UNIVERSITY Health Data Nova Scotia **Privacy Incident and Breach 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 14***

1. BACKGROUND & PURPOSE

1.1. The purpose of this policy is to guide Health Data Nova Scotia (HDNS) personnel and approved users of HDNS data on how to proceed in the event of a privacy incident or breach, and to demonstrate to stakeholders that a systematic procedure is in place to respond to and deal with privacy issues.

2. APPLICATION

2.1 This policy and protocol applies to breaches of privacy involving data housed by HDNS for research or health service assessment projects.

2.2 This policy applies to suspected and confirmed privacy incidents and breaches.

2.3 The protocol is divided into areas of responsibility for the person(s) discovering the breach (Discoverer) and /or HDNS personnel or contractor.

2.4 This policy does <u>not</u> apply to privacy incidents or breaches that do not involve HDNS data (e.g. personal information of personnel or requestor(s)). Concerns regarding these types of situations should be directed to the HDNS Manager.

3. DEFINITIONS

3.1 *Containment*: In the event of a breach, the processes put in place to prevent further release of information.

3.2 *Discoverer*: the HDNS personnel who suspects or discovers a breach or is the person told about the breach by someone other than HDNS personnel.

3.3 *External Breach*: refers to a breach that occurs from outside of HDNS (e.g. computer being hacked).

3.4 *Internal Breach*: a breach that occurs within the confines of HDNS.

3.5 *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.

3.6 *Privacy Breach*: A privacy breach occurs when there is an unauthorized access, use, disclosure, copying, modification, retention or destruction of personal health information.

3.7 *Privacy Incident*: a situation where the potential exits that a breach could occur but the situation was addressed before a breach occurred.

3.8 *Unique Identifiers*: Information that can directly identify an individual and includes: name, street address and identifying numbers (e.g., health card number, physician identification number, employee ID, Social Insurance Number).

4. POLICY STATEMENT

4.1 HDNS is committed to protecting the privacy, confidentiality and security of the personal health information (PHI) in its datasets and has policies and procedures designed to prevent a privacy breach. All authorized personnel and approved users will receive privacy, confidentiality and security training which include the process for handling a suspected or confirmed breach.

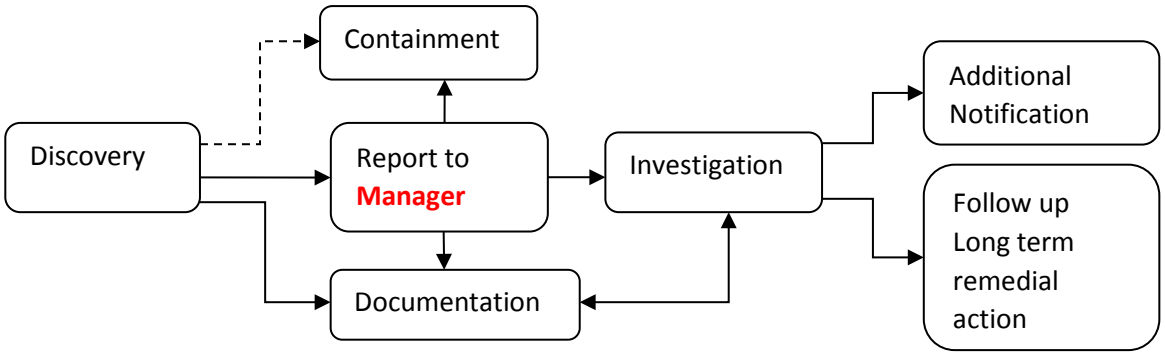
4.2 A privacy incident will be treated as a breach until it is ascertained that there was no unauthorized access, use, disclosure, copying, modification, retention or destruction of PHI.

5. PRIVACY INCIDENT AND BREACH MANAGEMENT PROTOCOL

5.1 The protocol outlined below is to be followed for both privacy incidents and breaches:

(1) Discovery and Reporting
(2) Containment
(3) Documentation and Investigation
(4) Additional Notification
(5) Follow up and Long-term Remedial Action

Note: Steps 1-3 should occur simultaneously or in quick succession.



--- if has ability to contain

Manager responsible to conduct and/or delegate activities

Step 1- Discovery and Reporting

5.1.1 All HDNS authorized users are required to **immediately** report the discovery of a privacy incident / breach (suspected or confirmed) to:

- their direct supervisor; and/or
- the HDNS Manager or, in their absence, the Dalhousie University Department Head, Community Health & Epidemiology, or their designate.

5.1.2 If an incident / breach is suspected or discovered by a non-HDNS authorized user they must report it to any HDNS authorized user present at the time, or the HDNS Manager. The HDNS authorized user must verbally notify the HDNS Manager immediately (in person or by phone).

5.1.3 The discoverer will document and include the following information in the **HDNS Privacy Incident / Breach Form**

- Project title and number (if relevant).
- Date and time of discovery.
- Who was involved (if known).
- Estimated date and time privacy incident/ breach occurred (if possible to estimate).
- Type of privacy incident / breach (e.g., unsecured password, loss, theft, inadvertent disclosure, maintenance of data past destruction, etc.) The discoverer describes the situation but does not make the determination whether the situation constitutes an incident or a breach.
- Type of data involved (e.g., Unique Identifiers, encrypted data).

5.1.4 The HDNS Manager will decide whether the incident meets the definition of a privacy breach. If it is determined to be an incident, the HDNS Manager will ensure that the Privacy Incident / Breach Form is completed and signed and then continue to Step 5. The HDNS Manager will notify the Nova Scotia Department of Health and Wellness (DHW) of the Incident once the internal process is complete.

5.1.5 If it is determined that a privacy breach occurred, the HDNS Manager will immediately report the breach to the Director, Health Privacy and Access at the DHW.

Step 2 – Incident / Breach Containment

5.1.6 Containment is to be initiated as soon as possible to prevent release or further release of personal health information.

5.1.7 The objectives of the containment process are to:

- Determine what, if any, information has been disclosed.
- Retrieve as much of the breached information as possible (ideally all breached information).
- Ensure no copies of the PHI have been made or retained by the individual who was not authorized to retrieve or receive the information (if possible).
- Ensure that additional breaches cannot occur through the same means.
- Determine whether the privacy breach would allow unauthorized access to any other personal information and take whatever necessary steps are appropriate (e.g. change passwords, identification numbers and/or temporarily shut down a system – if authorized), ensure evidence is preserved.
- Document all above information and be prepared to review with the HDNS Manager and / or the DHW.

5.1.8 The following steps illustrate the minimum actions required to contain the breach or suspected breach:

- If an electronic data device is stolen from the HDNS office, notify Dalhousie University security immediately to determine if the person who removed the device is still in the building.
- If a fax was sent to the wrong number, call the recipient and ask them to destroy the document and any copies that were made.
- If an email was sent to the wrong person, call the recipient and ask them to securely destroy any email printouts that were made and delete the email.

- If an unauthorized person has or may have access to a database or computer system, notify the System Administrator, who can disable accounts or change passwords and identification numbers.
- Where unauthorized verbal disclosure has occurred, request that the recipient of the personal or sensitive information treat it confidentially.

Step 3 – Documentation and Investigation

5.1.9 The discoverer reporting the incident / breach must document all the information on the **HDNS Privacy Incident / Breach Form** (attached) and provide the form to the HDNS Manager.

5.1.10 Once the HDNS Manager has completed the investigation s/he must complete the DHW Privacy Breach Reporting Form (attached).

5.1.11 The HDNS Manager must sign the completed DHW Privacy Breach Reporting Form and fax a copy to the DHW Health Privacy Office.

5.1.12 The HDNS Manager will assist the DHW Health Privacy Office in the conduct of the investigation as requested and follow any direction required.

Step 4 – Additional Notification

5.1.13 All external privacy breaches will be immediately reported to the Department Head of Community Health and Epidemiology and Dalhousie University Legal Counsel.

5.1.14 In discussion with the DHW Health Privacy Office, further notification processes (if any) will be determined. HDNS will comply with DHW direction regarding notification.

5.1.15 If the breach is found to have been intentional or the result of grossly negligent work practices, the appropriate person who has disciplinary authority over the person(s) responsible for the breach will be contacted to determine the appropriate disciplinary actions and/or consequences. The HDNS Manager will follow the process in the **Dalhousie University Scholarly Misconduct Policy** (attached).

Step 5 – Follow up and long term remedial action

5.1.16 Upon completion of the Investigation, a plan will be developed to prevent similar incidents/ breaches in the future (prevention plan):

- Determination of whether the privacy incident / breach protocol was followed.
- An education awareness piece to educate authorized and approved users on how to avoid similar incidents/ breaches.
- Review policy to ensure privacy and security requirements are clear.
- Review the privacy and security training program and documentation to identify and rectify gaps.

5.1.17 HDNS may reserve the right to disallow access to HDNS data for persons who have been the cause of a privacy breach / incident.

6. ADMINISTRATION

6.1 Accountability

6.1.1 All HDNS authorized personnel and approved users are responsible to immediately report an incident of suspected or confirmed breach of privacy / security to the appropriate person and follow the protocol as the Discoverer of the breach.

6.1.2 HDNS authorized personnel and /or the HDNS Manager are responsible to ensure proper containment of the breach; provide appropriate notification; document and report; take action to prevent future breaches and follow up with monitoring and audits.

6.1.3 The HDNS Manager is responsible to report the breach to the Health Privacy Office at the DHW, ensure all appropriate documentation is completed and signed, assist with the investigation as required, notify others as required and conduct the review and develop and /or implement the remedial plan.

6.2 Monitoring, auditing and reporting

6.2.1 All privacy incidents and breaches are logged and included an annual report to the DHW.

6.2.2 A copy of the completed **HDNS Privacy Incident / Breach Form** and the **DHW Privacy Breach Reporting Forms** is filed and retained indefinitely years.

6.2.3 Following any privacy breach investigation, this policy is reviewed to determine effectiveness and revised accordingly.

6.2.4 The Remedial Plan noted in Step 5 will include a requirement for an audit to ensure that the plan has been fully implemented.

7. RELATED POLICIES AND OTHER DOCUMENTS

7.1 HDNS Policies and Procedures

- HDNS Complaints Policy

7.2 HDNS Forms

- HDNS Privacy Incident / Breach Reporting Form

7.3 Other Documents

- Nova Scotia Department of Health and Wellness Privacy Breach Reporting Form
- Dalhousie University Scholarly Misconduct Policy

Nova Scotia Department of Health and Wellness:
Privacy Breach Reporting Form

This form is to be used to document the theft, loss or unauthorized access, use, disclosure, copying or modification of an individual's personal health information.

Please complete this document and provide the completed and signed document to:

Privacy and Access Office
NS Department of Health and Wellness
4th. floor Barrington Tower
1894 Barrington Street
Halifax NS B3J2A8
902-424-3573
Fax: 428-2267
Email: Elizabeth.iwaskow@gov.ns.ca

Note: When completing this form, include the minimum amount of personal health information necessary to adequately explain the breach. Do not include specific details please just describe the type of information that was allegedly breached (e.g. "the individual's diagnosis was included in the information").

Reporting

1. **Breach of:**
   - ☐ **Personal Health Information**
   - ☐ **Personal Information**

2. **Date and time of breach**

3. **Name and position of person who reported the breach**

4. **Details of the breach** (please include details concerning the type of information breaches, how it was discovered, the location, cause, and contact information for the individuals whose information was breached if known)

5. **If known, name and position of person(s) responsible for the breach**

Containing the Breach

Describe the steps taken to contain the breach. This may include recovering copies of information in all media and removing access privileges to persons allegedly involved in the breach. Include the names and positions of all persons involved in containing the breach. Attach all relevant documents.

SIGNATURES

Signatures

Note: Signatures may be required from the individual who reported the breach, his/her supervisor, the individual responsible for investigating the breach, and/or the Contact Person.

Include the dates the document was signed by each person.

Completed by Date

Employee responsible for breach Data

Supervisor/ Manager Date

TO BE COMPLETED BY THE DHW HEALTH PRIVACY OFFICE

Investigation of the breach

Outline all information related to the investigation of the breach. Attach all relevant documents.

Notification

Please Complete the Breach Notification Tool

Determination of whether notification is required

Will notification be made to the individual(s)?

- ☐ Yes
- ☐ No

If **"yes"**, outline how the notification will be made (e.g. phone call, letter), and by whom. Attach all relevant documents.

Notification – Individual

Include all relevant information including date and time of notification to the individual, and detailed notes of all discussions. Attach all relevant documents.

Follow-up

Outline any follow-up requested by the individual(s), or committed to by the person notifying the individual(s).

If **"no", ** outline the rationale for not notifying the individual. Include information on who participated in the decision. Attach all relevant documents.

Notification – Review Officer

If the decision has been made not to notify the individual, section 70(2) of the *Personal Health Information Act* requires that the custodian notify the Review Officer as soon as possible. **Attach a copy of the notification to the Review Officer.**

Privacy Breach Considerations Table

The following table is intended to help the DHW organize and summarize relevant, important elements/factors of the particular privacy breach circumstances under consideration. It is not a substitute for use of the tool's process steps to analyses the breach circumstances and to make a decision regarding notification of the breach subject/SDM or the Review Officer.

Program Area Affected: _____ Date: _____

File #: _____

Participants: _____

_____

_____

_____

_____

_____

Consideration	Particulars	Check all that apply
Type of Information	Relevant demographics	
	Health card number	
	Financial	
	Other type(s) of personal health information (PHI)	
Scope of breach	Number of affected or potentially affected breach subjects	
	Length of time from the breach to its discovery	
	Number of known or potential recipients of the PHI	
	Number of times the PHI was breached	
Method of Breach	Electronic system access	
	Verbal Disclosure	
	View only	
	Fax	
	Email/Electronic transfer	
	Lost/stolen	
	Incorrect mailing address	
	Social media	
	Hacking	
	Laptop	
	USB	
Recipient(s)	Agent/employee of the DHW	
	Another custodian	

	Unauthorized family member	
	Media	
	Regulated health professional	
	Individual member of the general public	
	Multiple members of the general public	
	Unknown (lost/stolen)	
	Friend or acquaintance	
Circumstances	Unintentional access or disclosure	
	Intentional access/use without authorization	
	Intentional disclosure without authorization	
	Loss	
	Malicious intent	
	For personal gain	
	Theft (targeted)	
	Theft (untargeted)	
	Existing relationship between person who breached information and the breach subject	
Disposition (what happened to the information after the breach)	View only with no further access or disclosure	
	Returned in full	
	Confirmation of proper destruction in timely manner (e.g. shredded, deleted)	
	Unable to retrieve electronically or in paper	
	Unsure of location of information	
	Re-disclosed (e.g., to media, social media, other person)	
Safeguards	Data encrypted	
	Password protected	
	Password protected but easily overwritten	
	No controls	
	PHI requires specialized knowledge to interpret	
Anticipated Impact(s)/ Burden(s) of Notification to the DHW	Resources – human	
	Resources – financial	
	Implications for (future) 'trust' in health professionals/organization	

**** For the complete "Breach Notification Decisions Making Tool" please contact the DHW Privacy and Access Office**