Leadership. Services. Support.

HEALTH ASSOCIATION NOVA SCOTIA

PERSONAL HEALTH INFORMATION ACT

Toolkit for Home Support Agencies in Nova Scotia

April 2014

2 Dartmouth Road

Bedford, Nova Scotia

B4A 2K7

INSERT CUSTODIAN'S
LOGO HERE

April 2014

This Toolkit is intended to provide a general explanation of the Personal Health Information Act and to provide resources to support its implementation in the Home Care Sector. This toolkit should not be used in the place of legal consult. Custodians are encouraged to seek legal counsel for advise specific to their circumstances. Several of the resources included have been taken or adapted from the Department of Health and Wellness' Toolkit. In the event that there is a discrepancy between this document and the Personal Health Information Act and its Regulations, the latter should be considered the authoritative text.

Complying with the Personal Health Information Act in Homecare Toolkit

Table of Contents

List of Tools & Templates

- Master Checklist
- Notice of Purposes Template
- Written Privacy Statement Template
- Retention & Destruction Schedule Template
- Destruction, Disposal & De-identification Checklist
- Substitute Decision Maker Hierarchy, Selection Criteria and Decision-Making Guide
- Privacy Complaint Policy Template
- Privacy Complaint Form
- Privacy Breach Reporting Policy
- Safeguards for Electronic Records
- Personal Health Information Breach Reporting Form
- Request for Access to Personal Health Information: Policy
- Request for Access to Personal Health Information: Request Form
- Estimate of Fees – Access to Personal Health Information
- Request for Access to Personal Health Information: Response Form
- Request for Correction to Personal Health Information: Policy
- Request for Correction to Personal Health Information: Request Form
- Request for Correction to Personal Health Information: Response Form
- Indirect Collection of Personal Health Information Checklist
- Limiting/Revoking Consent Request Form
- Limiting/Revoking Consent Response Form
- Research Plan Checklist
- Review Officer Notification
- Data Disclosure Agreement
- Request for Access to Personal health Information for Researchers form
- Consent Matrix

Master Checklist for PHIA Compliance

Has my organization developed, distributed and implemented as appropriate, the following:

- ☐ Designated a PHIA contact person
- ☐ Notice of Purposes
- ☐ Written Privacy Statement
- ☐ Retention & Destruction Schedule
- ☐ Privacy Complaints Policy
- ☐ Ability to Report Privacy Breach (e.g. Privacy Breach Policy)
- ☐ Ability to Produce a Record of User Activity
- ☐ Ability to Produce and Maintain a Record of Security Breaches to Electronic Information Systems
- ☐ Administrative Safeguards to Protect Personal Health Information
- ☐ Physical Safeguards to Protect Personal Health Information
- ☐ Technical Safeguards to Protect Personal Health Information (For Electronic Records Only)
- ☐ Requests for Access to Personal Health Information
- ☐ Requests for Changes to Personal Health Information
- ☐ Disclosure of Personal Health Information Without Consent Reporting Form
- ☐ Process for clients to limit/ revoke consent for the collection use and/or disclosure of their personal health information

Designating a Privacy Contact Person

A custodian is required to designate a contact person under *the Personal Health Information Act (*herein referred to as PHIA*)* to enhance accountability.

Who can be a privacy contact person?
Although PHIA does not specify pre-requisites for the contact person, (s)he must have sufficient knowledge about their duties to be able to assist individuals who have questions about their personal health information and how it is managed by the custodian. The contact person must also understand the requirements in PHIA to a level that would support their training of the custodian's staff and providing information to the custodian's agents and to the public.

If appropriate, the custodian can take on the role of contact person. The duties of the contact person can also be shared by more than one person in the custodian's organization.

Another consideration in the designation of a privacy contact person is their role in the direct provision of care to clients, particularly with respect to receiving and processing complaints. Given a client may feel uncomfortable making a compliant to someone who directly provides their care, it may be prudent for custodians to make the contact person someone who is not involved in the direct provision of care to clients, or at least assign the duties of overseeing complaints to a non-care provider.

What are the responsibilities of a privacy contact person?

- facilitate the custodian's compliance with the *Act;*
- ensure that all agents of the custodian are informed of their duties under the *Act*;
- respond to inquiries about the custodian's information practices;
- respond to requests for access to and correction of records;
- receive and process complaints under the *Act*;
- facilitate the communications and the training of the custodian's staff about the custodian's policies and procedures and about the *Act*; and
- develop information to explain the organization's policies and procedures.

The name and contact information for the contact person must be included in all privacy notices and policies under PHIA. If more than one person is designated as being a *PHIA* contact, each contact person, their contact information and their duties under *PHIA* should be included. For example, if one person is responsible for responding to requests for access and correction, and another is responsible for all other duties under PHIA, both would be listed with their individual contact information and their specific duties.

Notice of Purposes under PHIA

Under the PHIA custodians are required to have a notice of purposes readily available for the client or, if the client lacks capacity, a substitute decision-maker. The notice of purposes describes the purpose of the custodian's collection, use and disclosure of personal health information.

The notice of purposes must contain enough information so the individual is able to understand why their personal health information is being collected, how it will be used, why it would be disclosed, and their individual rights under the Act.

The notice of purposes should include:

- A statement of the purpose of the Act, including the need to balance privacy rights of individuals, with the need for health professionals to use this information to provide appropriate care.
- A general statement about how the information will be used and disclosed, such as provision of health care, consultation with other providers, with students in training, to obtain payment for services, and to report issues required by provincial or federal law.
- A statement about the individual's rights under PHIA, and where the individual can make a complaint or ask for a review under the Act:
    - to request and receive or view a copy of the individual's personal health information (with exceptions)
    - to request that corrections be made to personal health information that is not accurate, complete, or up-to-date
    - to request a record of who has accessed the individual's personal health information on an electronic information system (a record of user activity)
    - to request that specific personal health information not be provided to other health care providers
    - to be advised if a breach of the individual's personal health information has occurred
    - to make a complaint to the custodian about a concern related to access, correction or another privacy issue under the *Act*, and where to make that complaint
    - to request a review by the Review Officer of the custodian's decision or actions

The notice of purposes must be readily available, in a location where the client or substitute decision maker can easily locate and read it. Given the nature of home care services do not allow for one centralized location where clients regularly go, such as a waiting room, providing the notice of purposes at the first visit between the home care agency and the client is acceptable.

The notice of purposes is a mechanism for custodians to infer knowledgeable implied consent. Knowledgeable implied consent is the consent required to provide care. In order for knowledgeable implied consent to be inferred, it must be reasonable for the custodian to think that individual understands the purpose of the collection, use and disclosure of their health information. This can be achieved through the notice of purposes, assuming it meets the criteria listed above, or through explaining directly to the individual. A custodian cannot infer knowledgeable implied consent when the custodian should have known that the individual has a limited ability to understand the notice (e.g. language barriers, a disability or condition that would impair understanding of the notice). There are exceptions when express consent, rather than knowledgeable implied consent is required, and when no consent is required (see **consent matrix on page 74**).

A Notice of Purposes Template can be found on page 25.

Written Privacy Statement

Under the PHIA, section 68, custodians must have a written privacy statement made available to the public. The written privacy statement is a more detailed version of the notice of purposes. It must be available to the public on request. In home care, this could include providing brochures to clients and/or posting this written privacy statement on the custodian's website. The written privacy statement must explain:

- the custodian's information practices
- how to contact the designate contact person
- how to obtain access to or request correction of a record
- how to make a complaint

The written privacy statement may provide information in addition to the notice of purposes, such as expectations around timelines for complaints, access and changes to personal health information.

See written privacy statement template on page 26.

Retention and Destruction of Personal Health Information

Under the PHIA, custodians are required to have a written retention and destruction schedule for *identifying* personal health information. The schedule must provide legitimate purposes for retaining the information, and retention/destruction schedules corresponding to each purpose.

Retention: Personal health information, should generally be retained for only as long as is needed to fulfill purposes, yet long enough to allow an individual to access the information and challenge the accuracy of a decision (e.g. level of need). An individual's right of access to personal health information continues until personal health information has been destroyed in accordance with a destruction/disposition schedule. Retention schedules should include a minimum and maximum retention time and consider all forms of media on which client information is stored (i.e. paper, electronic, microfiche) (see retention and destruction schedule template). In setting timelines for retention and destruction, the custodian should consider any pre-existing guideline or (e.g. a service agreement between the home care agency and a district health authority, regulatory bodies which have provided guidance on retention of records, Canada Revenue Agency for financial records, etc.).

Under section 49(3) custodians can retain *de-identified* information form to be used for secondary purposes, including research.

Destruction, erasing or de-identifying of personal health information must be done so in a secure manner, so that "reconstruction is not reasonably foreseeable in the circumstances" (e.g. cross-cut shredding of paper documents, or wiping the hard drive of electronic records). A custodian should also be cognizant of duplicate copies of the information that might exist, such as on hard drives of office equipment (e.g.

photocopiers and fax machines). De-identified information, means the information has been removed of anything that directly identifies the individual (e.g. name), and it is not reasonably foreseeable in the circumstances that the information, alone or with other information can identify the individual. Once information is de-identified, PHIA no longer applies, nor does it apply to statistical or aggregate health information. These types of information can therefore be retained or destroyed outside of the retention schedule.

See retention and destruction schedule template on page28.

A destruction, disposal and de-identification checklist can be found on page 29.

Capacity and Substitute Decision Makers

Capacity and substitute decision-making is especially relevant in the home care sector, given many clients face, or will soon face cognitive difficulties.
Under PHIA capacity means:

- The ability to understand information that is relevant to the making of a decision related to the collection, use or disclosure of personal health information, and,
- The ability to appreciate the reasonably foreseeable consequences of a decision or lack of decision.

Where an individual lacks capacity to consent to the collection, use and disclosure of their personal health information, a substitute decision maker can make that decision on the individual's behalf. There can be different substitute decision makers for different custodians and/or different circumstances (e.g. an individual may lack capacity for some decisions and not others).

A hierarchy of substitute decision-makers, criteria for selecting substitute decision makers, and considerations for decision-making can be found on page 30.

Privacy Complaints under PHIA

Custodians must implement, maintain and comply with a complaints policy outlining how an individual can make a complaint regarding the custodian's conduct in relation to privacy provisions under PHIA, which are the following:

- Consent
- Substitute decision makers
- Collection, use, and disclosure of personal health information
- Retention, destruction, disposal and de-identification of personal health information
- Research
- Practices to protect personal health information
- Reporting of a privacy breach

Under PHIA *Regulations*, the complaints policy must:

- State that an individual must submit a complaint to the custodian in ***writing***; and
- State the time period during which the custodian must process, investigate, make a decision on the complaint and reply to the complainant.
- Complaint response times are as follows:
    - Within 60 days - Standard
    - Within 90 days as long as written notice is given to complainant within 60 days
    - 90+ days, only with the permission of the Review Officer, and if the following apply:
        - Replying to the complaint within the 30-day extension period would unreasonably interfere with the activities of the custodian
        - The time required to undertake the consultations necessary to reply to the request within the 30 day extension period would make it not reasonably practical to reply within that time.

According to the Act, an individual must go through the internal complaint process before initiating a review with the Review Officer.

A Privacy Complaint Policy template can be found on page 31.

A Privacy Complaint Form can be found on page 33.

Privacy Breaches

Under PHIA a custodian is required to notify the breach subject at the "first reasonable opportunity" if it is reasonable to believe that:

- the information is stolen, lost or subject to unauthorized access, use, disclosure, copying or modification; **AND**
- as a result, there is potential for harm or embarrassment to the individual.

If no there is no risk of harm or embarrassment the custodian does not have to notify the individual, however they must notify the review officer. Although PHIA does not require custodians to have a privacy breach reporting policy, a policy and procedure template has been developed for custodians to use at their discretion (see **Privacy Breach Reporting Policy template on page 36**). The policy outlines steps to be taken when a privacy breach occurs, and factors to consider in whether or not the breach subject should be notified. Factors which should be considered during the investigation of the breach and in determining whether or not the breach subject should be notified are listed below[1].

- **Type of information breached and degree of sensitivity**
- **Scope of breach** (# subjects and recipients of breach, length of time, # of breaches)
- **Method** (e.g. hacking/theft vs. incorrect email/fax)
- **Recipient(s)** (e.g. agent vs. media/public)
- **Intent** (accidental vs. malicious)
- **Disposition** (returned/destroyed vs. further breached/unable to retrieve)
- **Safeguards** (none vs. encryption)
- **Anticipated impact of notification** (human, financial resources)
- **Scope of Harms**
    - Physical harm(s)
    - Psychological harm(s) including embarrassment, humiliation and threat to dignity
    - Financial/economic burdens
    - Identity theft and/or fraud
    - Reputational harm (damage to the breached subject's reputation)
    - Basis(es) for potential discriminatory action(s) that may be taken against the breached subject
    - Social/relational harm (damage to the breached subject's relationships)

For Electronic Records Only:

The *PHIA* regulations state that:

"A custodian shall create and maintain a record of every security breach of the custodian's ***electronic information system*** *that the custodian determines on a reasonable basis is likely to pose a risk to an individual's personal health information*. (*PHIA* regulation section 10 (3))

A record of security breaches must include details of all corrective procedures taken by the custodian to diminish the likelihood of future security breaches." (*PHIA* regulation section 10 (4))

A Privacy Breach Reporting Policy Template can be found on page 36.

A Privacy Breach Reporting form can be found on page 39.

[1] Criteria taken from Privacy Breach Notification Decision-Making Tool developed in collaboration between the Nova Scotia Department of Health and Wellness and the Nova Scotia Health Ethics Network.

Safeguarding Personal Health Information

Under PHIA regulations custodians are required to implement additional safeguards for electronic information systems holding personal health information maintained by the custodian. These additional safeguards are:

- protection of network infrastructure, including physical and wireless networks, to ensure secure access;
- protection of hardware and its supporting operating systems to ensure that the system functions consistently and only those authorized to access the system have access;
- protection of the system's software, including a mechanism to authenticate a user's identity before allowing access, such as user names and passwords. (PHIA regulation section 10 (1))

In addition, a "*custodian must create and maintain written policies to support and enforce the implementation of the safeguards…*" (*PHIA* regulation section 10 (2)).

Ensuring that personal health information is protected requires the successful integration of three types of security measures:

- administrative safeguards;
- physical safeguards; and
- technical safeguards.

Administrative and physical safeguards can be applied to paper records as well as electronic records. **Examples of the three types of safeguards, including those that are required can be found in on page 42**. Although not all of these safeguards are required by PHIA, this can be used as a checklist to do a privacy audit to determine the breadth of safeguards the custodian has in place. This can allow a custodian to determine if there is one area which may be lacking and where their vulnerabilities and risks may lie.

Administrative safeguards are particularly important, as even the most robust physical and technical safeguards can be compromised if agents are not aware of information policies and practices, or do not abide by them. These may include the establishment of appropriate security policies enforcement and adequate training and education of staff, volunteers, contractors and other agents.

Custodians may choose to conduct a risk assessment of all their electronic information systems to evaluate the potential risks and vulnerabilities to the privacy, confidentiality and integrity of the personal health information. Once conducted, custodians can then consider how best to implement the administrative, physical, and technical safeguards necessary to adequately protect the personal health information. Factors to consider may include the sensitivity of the information, the risks associated with exposure of the information, the size of the organization, the number of users of the system.

Record of User Activity

Under PHIA, individuals have the right to request a list of users who have accessed their personal health information for any ***electronic information system*** the custodian uses to maintain the individual's personal health information.

The record of user activity must be made available within 30 days and free of charge.

Under PHIA regulations, the record of user activity must include at minimum:
• the name of the individual whose personal health information was accessed;
• a unique identification number for the individual whose personal health information was accessed, including their health-card number or a number assigned by the custodian to uniquely identify the individual;
• the name of the person who accessed the personal health information;
• any additional identification of the person who accessed the personal health information, including an electronic information system user identification name or number;
• a description of the personal health information accessed or, if the specific personal health information accessed cannot be determined, all possible personal health information that could have been accessed;
• the date and time the personal health information was accessed or, if specific dates and times cannot be determined, a range of dates when the information could have been accessed by the person.
Custodians may also consider capturing the following elements if they have the capacity to do so:
• the location of the user where the information was accessed;
• the specific action performed or conducted by the user (e.g. viewing, modifying, deleting, printing, editing, signing off, writing); and
• the length of time the action took place.

Given that not all custodians have (or should have) an elaborate electronic information system with robust audit functionality, the regulation allows for a broad response to the specific type of personal health information accessed along with ranges for the dates and times. Therefore, custodians unable to extract this information electronically from their electronic information system are still able to comply with the regulation by providing a more general description. This information may be captured through the custodians scheduling system (date and time) along with a detailed list of the personal health information captured by the applicable system.

Note: there is a distinction between an "audit log" and a "record of user activity". The audit log may or may not contain more fields than those required by regulation to produce a record of user activity.
A record of user activity may be generated by taking specific fields from a system's audit log and forming a report that could be provided to an individual. The PHIA regulations require that the audit logs used to generate a record of user activity, if they exist, must be kept for at least one year from the date they were used to create a record of user activity (PHIA regulation section 10(2)). A custodian will determine the retention period for the audit logs on an ongoing basis and this can be included in their written policies.
Under PHIA custodians are not required to produce an audit log, however an audit log can help in the production of a record of user activity.

Requests for Access to Personal Health Information

Under *PHIA* an individual has the right to access a record of their personal health information. In order for an individual to request access to their personal health information:

- The request must be made in writing to the custodian of the personal health information
- The request for access must specify the subject matter of the record requested with sufficient information to enable the custodian to locate the record
- The individual must pay any required fees (unless waived by custodian)
- **The individual does not have to provide the reasons or purposes for which they are requesting the information**.

In response to a request for access to personal health information, a custodian must:

- Respond, in writing, **no later than 30 days** after receiving the request. In the written response, the custodian must either grant the request, refuse the request, or extend the deadline.
- Provide a fee estimate to the individual
    - The final fee payable may be altered in compliance with the regulated fee schedule if the actual cost to the custodian were higher (e.g., estimated the record would be 50 pages, but was actually 75)
    - The fee should not be a barrier to access
    - The custodian has the discretion to waive all or part of an access fee
- If a request is refused, the custodian must notify the individual in writing, justifying why the request was refused, and also inform the individual that (s)he has the right to make a complaint to the Review Officer

A Request for Access to Personal Health Information Policy Template can be found on page 44.

A Request for Access to Personal Health Information Form can be found on page 46.

An Estimate of Fees - Access to Personal Health Information Form can be found on page 47.

A Request for Fee Waiver-Access to Personal Health Information Form can be found on page 49.

A Response to Request for Access to Personal Health Information Form can be found on page 50.

Requests for Correction of Personal Health Information

Under PHIA an individual may request that a custodian corrects information contained within their records of personal health information. **A fee cannot be charged for this**.

The custodian is not required to correct a record if:

- it consists of a record that was not originally created by the custodian and the custodian does not have sufficient knowledge, expertise, and authority to correct the record; or
- it consists of a professional opinion or observation that a custodian has made in good faith about the individual (section 87(2)).
- A custodian may also refuse to correct a record where the custodian believes on reasonable grounds that the request for correction is frivolous or vexatious or suggests a pattern of conduct that amount to abuse of the right to correction.

A custodian who receives a request for correction must respond, in writing, as soon as possible, **no later than 30 days** after receiving the request. In the written response, the custodian must either grant the request, refuse the request, or extend the deadline.

A Request for Correction to Personal Health Information Policy Template can be found on page 53.

A Response to Request for Correction to Personal Health Information Form can be found on page 55.

Collection, Use & Disclosure of Personal Health Information

- A custodian cannot collect, use or disclose personal health information where other information will serve the custodian's purpose; and
- A custodian must collect, use and disclose the minimum amount of personal health information necessary to achieve the custodian's purpose.

Collection

PHIA defines "collect" in relation to personal health information as, "to gather, acquire, receive, gain access to or obtain the information by any means from any source" (section 3(c)).

Custodians must collect personal health information directly from the individual about whom the information is being collected. **Circumstances under which indirect collection is permissible can be found on page 57.**

Use

PHIA defines "use" in relation to personal health information in the custody or control of the custodian as to handle or deal with the information (section 3(ab)).

Where the *Act* permits a custodian to collect personal health information, section 33 also permits the custodian to use the information for:

- the purpose for which the information was collected or created and for all the functions reasonably necessary for carrying out that purpose;
- a purpose for which this *Act*, another *Act* of the Province or of the Parliament of Canada permits or requires a person to disclose it to the custodian;
- educating agents to provide health care.

If an individual determines that they do not want their personal health information used for a specific purpose (e.g. educating students) they have the right under *PHIA* section 17 to request that it not be used for that purpose. However, an individual cannot request that a custodian not use information that is required by law to be disclosed to the custodian (e.g. where this disclosure is required by law, treaty, agreement or arrangement made pursuant to this Act, or another provincial or Federal Act).

Disclosure

Under PHIA "disclose" in relation to personal health information in the custody or control of a custodian is defined as making the information available or releasing it to another custodian or to another person (section 3(h)).

Generally speaking, the stipulations for disclosing personal health information are more stringent than for collecting and using personal health information.

Disclosure of personal health information without the individual's consent must be documented and include the following (a **Disclosure of Personal Health Information without Consent Form can be found on page 58).**

- A description or copy of the personal health information disclosed
- The name of the person or organization to whom the personal health information was disclosed
- The date of the disclosure
- The authority for the disclosure (e.g. treaty/agreement, provision under this Act or another Act)

In the case where a custodian may disclose personal health information to a non-custodian for the purposes of facilitating assessment, care and treatment services for the individual, before the information may be disclosed:

- The custodian must make a request to the Minister in writing detailing the reason why the non-custodian requires the personal health information on an ongoing basis, and have that request authorized by the Minister of Health and Wellness.

Under PHIA, knowledgeable implied consent for disclosure of personal health information can be assumed within the circle of care.

Circle of Care

The circle of care refers to the custodians who provide or support care to an individual in each instance of care provision. The circle of care allows for information to flow under a different set of rules, whereby those included in the circle of care may assume knowledgeable implied consent to collect use or disclose personal health information for the purpose of providing health care, unless a custodian knows that an individual has expressly withheld or withdrawn consent. Information may only be disclosed by a custodian to another custodian (or their agent) within the circle of care. If an organization or health provider that is not a designated custodian under PHIA falls within the circle of care, express consent from the individual must be obtained from the individual. It is important to note that those that fall within the circle of care can change based on each instance of care provision.

Under section 37 of PHIA, a custodian has the discretion to disclose personal health information related to the **presence, location and general condition of an individual** on the day that the information is requested to:

- family members of the individual; or
- another person if the custodian has a reasonable belief that the person has a close personal relationship with the individual.
- **A custodian may not disclose this information if it is contrary to the express request of the individual**.

Under section 40(2), a custodian may disclose personal health information about a **deceased individual if the information relates to circumstances surrounding the death of the individual or to health care recently received by the individual** and the disclosure is not contrary to a prior express request of the individual, to:

- a family member of the individual; or
- another person if the custodian has a reasonable belief that the person has a close personal relationship with the individual.

Under section 40(1), a custodian may release information about an **individual who is deceased, or believed to be deceased**, for the following purposes:

- for the purpose of identifying the individual;
- for the purpose of informing any person whom it is reasonable to inform that the individual is deceased or believed to be deceased;

- to a spouse, parent, sibling, or child of the individual if the recipient of the information reasonably requires the information to make decisions about the recipient's own health care or the recipients children's health care and it is not contrary to a prior express request of the individual;
- for carrying out the deceased person's wishes for the purpose of tissue or organ donation.

Consent for the Collection, Use and Disclosure of Personal Health Information

There are 3 different models of consent pertaining to the collection, use and disclosure of personal health information (**see Consent Matrix on page 57** for an explanation for each of the models of consent for each of the personal health information activities). The models of consent are:

Express Consent	Although not explicitly defined in PHIA, express consent should be voluntary, not require inference on part of the custodian and can be verbal or written
Knowledgeable Implied Consent	For Knowledgeable Implied Consent to be inferred: • The individual must know the purpose of the collection, use of disclosure, as the case may be; and • The individual must know that s/he may give or withhold consent • The custodian must either provide verbal or written information directly to the individual, post a notice of purposes or distribute brochures that are readily available to the public If the individual proceeds to pursue services knowledgeable implied consent can be inferred.
No Consent	See consent matrix for circumstance where consent is not required

Where consent (express or knowledgeable implied) is required, it must meet the following requirements:

- It must be given by the individual or the substitute decision-maker if the individual lacks capacity
- It must be knowledgeable
- It must be related to the specific information at issue; and
- It must be voluntary

Further considerations for Knowledgeable Implied Consent:

While a notice of purposes is typically sufficient for knowledgeable implied consent, the custodian cannot infer that the individual understands the purposes if the custodian should have known that:

- the individual has a limited ability to read or understand the language in which the notice or explanation is presented; or
- has a disability or condition that impairs the individual's ability to read or understand the notice.

If this is the case, section 15(3) requires the custodian to make "reasonable efforts" to assist with the individual's understanding of the purposes. This may include verbally explaining the purpose(s) to the individual, or facilitating an explanation – verbally or in writing - in the individual's language.

Limiting/Withdrawing Consent

An individual may request to limit or revoke consent for the collection, use or disclosure of their personal health information by giving notice to the custodian (section 17(1)), however this is not applied retroactively. For example, if an individual informs a custodian that s/he is withdrawing consent to have information disclosed to one of his/her health providers, the custodian is not required to request that any information previously disclosed to the other provider be returned.

When consent for collection, use or disclosure of personal health information is limited or revoked, a custodian must:

- inform the provider named by the individual that the individual's record is not complete, meaning the custodian considers that the information disclosed to that provider is not what is "reasonably necessary" for the care of the individual.
- inform the individual of the consequences of limiting or revoking consent (section 17(4)), including the fact that the other provider may decide that s/he is not confident in providing care to the individual without understanding what information has been withheld.
- take reasonable steps to comply with an individual's request to limit or revoke consent (section 17(3)). *In some circumstances it may not be possible to mask information due to technological capabilities*. The revocation of consent does not apply to collection, use and disclosure of personal health information that a custodian is required by law to collect, use or disclose (section 17(6)).

A Request to Limit/Revoke Consent Form can be found on page 59.

A Response to Request to Limit/Revoke Consent Form can be found on page 60.

Research

Pursuant to sections 55 and 56 of *PHIA* a custodian may *use* and/or *disclose* personal health information for research purposes in the following circumstances:

A custodian can **USE** PHI for research purposes if before commencing the research, the custodian:	A custodian can **DISCLOSE** PHI about an individual to a researcher if the researcher:
• prepares a research plan that meets the requirements in section 59; • submits the research plan to a research ethics board (REB); • receives the approval of the research ethics board; and • meets any conditions imposed by the REB.	submits to the custodian: • an application in writing; • a research plan that meetings the requirements of section 59; and • a copy of the submission to and decision of a research ethics board that approves the research plan; and enters into the agreement required by section 60. (data disclosure agreement)

Consent of research participants is still required unless a REB has determined that the consent of the subject individuals is not required, or that it is *impracticable* to obtain consent.

Impracticability

PHIA section 52(b) defines "impracticable" as *"a degree of difficulty higher than inconvenience or impracticality but lower than impossibility."*

Examples where obtaining consent may be impracticable:

- the size of the population being researched;
- the proportion of prospective participants likely to have relocated or died since the time the personal information was originally collected; or
- the lack of an existing or continuing relationship between prospective participants and the data holder who would need to contact them (e.g. a patient database that does not have a regular follow-up program to maintain a complete and accurate record of changes in registrants' contact information over time);

such that:

- there is a risk of introducing bias into the research because of the loss of data from segments of the population that cannot be contacted to seek their consent, thereby affecting the validity of results and/or defeating the purpose of the study; or
- the additional financial, material, human, organizational and other resources needed to obtain consent could impose a hardship or burden on the researchers or organization so burdensome that the research could not be done.

Researchers
The researcher requesting personal health information from a custodian must meet certain requirements.

In the case that consent of subject individuals will be obtained, the researcher must:

- Submit to the custodian
  - an application in writing;
  - a research plan that meets the requirements of Section 59; and
    a copy of the submission to and decision of a research ethics board that approves the research plan; and
- Enter in a data disclosure agreement.

These steps must take place before research is started.

In the case that consent of subject individuals will not be obtained:

- The researcher must meet the requirements listed above
- The research ethics board have determined that the consent of the subject individuals is not required;
- The custodian must be satisfied that:
  - the research cannot be conducted without using the personal health information;
  - the personal health information is limited to that necessary to accomplish the purpose of the research;
  - the personal health information is in the most de-identified form possible for the conduct of the research;
  - the personal health information will be used in a manner that ensures its confidentiality; and
  - it is impracticable to obtain consent; and
- **The custodian informs the Review Officer that personal health information is being disclosed without the subject individuals' consent.**

A *Research Plan Checklist* can be found on page 61
A *Review Officer Notification letter can be found on p. 62*
A *Data Disclosure Agreement* can be found on page 63
A *Request for Access to Personal health Information for Researchers* form can be found on page 65

Complying with PHIA in Home Care: Frequently Asked Questions

1. **Is my organization a custodian even if it didn't create the record containing personal health information? A lot of the information on home care client files originates from care coordinators in the districts, but some of the information comes from our home care agency. Are my duties and obligations different for information that my agency adds to the file, and the information that was added by another organization?**

   The originator or creator of the record is not relevant here. To be a custodian, the organizations have "custody or control" of the personal health information on the record. Regardless of who created the record, or who added information to the record, as long as the information is in the custody or control of the organization, that organization is considered a custodian. There can be multiple custodians for one file. For example, if a district health authority and a home care agency have a client's care plan and assessment, they are both custodians of this information, and are required to comply with PHIA.

2. **Does PHIA apply differently to private and for-profit home care agencies?**

   If a home care agency is approved by the Department of Health and Wellness and has a service agreement with a district health authority under the Health Authorities Act, or with the Izaak Walton Killam Health Centre, they must comply with PHIA, regardless of whether or not they are private, for-profit, or not-for-profit.

3. **Often our home care clients have files that they keep in their homes for their own use. Does PHIA apply to these records?**

   No. PHIA applies to personal health information that is under the custody or control of custodians. When a file is left in the client's home it is the responsibility of the client (competent) and or the Substitute Decision Maker (if client is not competent) to manage the access to the file.

4. **What should be taken into consideration when choosing a Privacy contact person? Is there anyone who should not be a designated privacy contact person?**

   A privacy contact person does not need to have any particular education or training. However if there is someone in the organization which has particular knowledge in the area, it makes sense for them to fill the role. Custodians may also want to consider if the contact person is someone who is involved in the direct provision of care to clients, at least for the purposes of receiving and handling privacy complaints. Clients may not feel comfortable making a complaint to someone who is directly involved in their care. A custodian may also want to consider the duration of the contact person's employment, for the sake of continuity (e.g. A custodian may not want to make a term or contracted position the privacy officer).

5. **How can I ensure that third party vendors and contractors we deal with are PHIA compliant?**
   PHIA does provide rules that govern third party recipients outside of the health sector who receive personal health information from a custodian (section 45).
   The third party recipient has a duty under the *Act* to not use or disclose the personal health information for any purpose other than:
   - the purpose for which the custodian was authorized to disclose the information under the Act; or
   - for the purpose of carrying out a legal duty.

   The recipient shall not use or disclose more of the information than is reasonably necessary to meet the purpose of the use or disclosure, unless the use or disclosure is required by law (section 45(3)).

6. **Where does PHIA not apply?**
   PHIA does not apply to:
   - de-identified health information, statistical or, aggregate health information, where the number is large enough for anonymity (e.g. aggregate data on a rare condition in a small area, where there are only two people making up the aggregate could still be considered identified health information).
   - personal health information about an individual, the earlier of 50 years after his/her death or 120 years after a record containing the information was created (section 5(2)(b)).
   - personal health information collected, used or disclosed outside of the health sector is not covered by *PHIA*. For example, insurance companies, employers, and regulatory bodies of health care professionals collect and use personal health information about individuals. However, they are not governed by *PHIA* because they did not have personal health information for the purposes of health care or the planning and management of the health system.

7. **How can Home Support Agencies distinguish between and deal with consent for service and consent to the collection, Use and/or disclosure of Personal Health Information?**

   Home Care Agencies that are approved by the DHW and have a service agreement with DHAs/IWK are considered custodians under PHIA, therefore, personal health information may be shared (i.e., between care coordinators employed by the DHAs and Home Support Agencies) as they would be within that individual's circle of care and knowledgeable implied consent could be relied upon. However agencies had previously been instructed to obtain direct consent from clients to deliver service. The Continuing Care Branch is aware of the PHIA change and will review policies, standards for any required changes.

8. **What is a sufficient level of care to protect the confidentiality of a client's personal health information, particularly during transport to and from clients' homes (e.g. Is it sufficient to have them locked in a car during transport to a client's home, or must they be "double locked" such as in a locked box or briefcase)?**

   Safeguards for protecting personal health information can be found on page 42. Safeguards explicitly required under PHIA are referred to with the corresponding section. It is up to the agency to determine what are safeguards are reasonable to have in place as there can be various ways to achieve and ensure the safe storage of files. Agencies need to look at best practice in the industry to ensure the outcome of secured files. Files should be with the employees at all time.

9. **While PHIA requires agencies to have a record retention and destruction policy, it does not specify the term of this. Does DHW have a specific requirement as it applies to LTC and to home care agencies?**

   This will vary depending on the nature of the records (e.g. Canada Revenue Agency references seven years for financial information to be retained). Service agreements between the DHAs and home support agencies require agencies to retain operational records for seven years following any termination or expiry of the Agreement. The Homes for Special Care Act references five years. The Act is scheduled for amendments this coming year and this gap (5 years) will be addressed.

Additional Resources
For additional information and resources regarding the Personal Health Information Act please see:
http://novascotia.ca/dhw/phia/

For additional information and resources on privacy laws in other jurisdictions please see:

http://www.ehealthontario.on.ca/images/uploads/pages/documents/InfoSecGuide_SmallOffices.pdf

https://www.infoway-inforoute.ca/index.php/about-infoway/privacy-mandate/privacy-faqs

http://www.ipc.on.ca/english/Home-Page/

http://www.healthinfoprivacybc.ca/

http://www.gov.mb.ca/health/phia/

http://www.oipc.ab.ca/pages/home/default.aspx

http://www.health.gov.sk.ca/hipa

http://www.gnb.ca/0051/acts/index-e.asp

http://www.health.gov.nl.ca/health/phia/

Tools and Templates

INSERT CUSTODIAN'S
LOGO HERE

April 2014

Notice of Purposes Template

Protecting your personal health information under the Personal Health Information Act

What is the Personal Health Information Act?	The *Personal Health Information Act* or *PHIA* is a new provincial law that aims to balance your right to have your personal health information protected with the need of those in the health sector to use your information to provide you with appropriate care and treatment.
How does PHIA protect my personal health information?	*PHIA* requires that "custodians" of personal health information (including hospitals, physicians, home care agencies and nursing homes) have policies and practices to protect your personal health information. Under *PHIA* we must: • follow *PHIA*'s requirements for appropriate collection, use, disclosure, retention and destruction of your personal health information • have a privacy contact person who can answer your questions about our management of your personal health information • have policies to protect the privacy and security of your personal health information whether it is held on paper or in electronic form, or if it is unrecorded • have a complaints policy for you to use if you have concerns about our compliance with *PHIA* • take appropriate action if the privacy of your personal health information has been breached which may include notifying you or the Privacy Review Officer • handle your requests for access to and correction of your personal health information
Who can see and use my personal health information?	• individuals involved in your care and treatment, including students • individuals who require the information to get payment for your health care • anyone who can legally act for you with your consent • specified organizations who have a legal right to see the information
What are my rights under PHIA?	You have the right to: • have your personal health information collected, used, disclosed, retained and destroyed according to the provisions in *PHIA.* • request access to your personal health information which is provided according to the *PHIA* access fee schedule • request a correction to your personal health information. • request information on who has accessed your personal health information held in electronic form. • request that some or all of your personal health information not be collected, used or disclosed to specific individuals or organizations involved in your care. • make a complaint to any custodian related to their management of your personal health information. • request a review by the Review Officer responsible for *PHIA* if you are not satisfied with the resolution of your complaint or your access or correction request.
Who do I contact for more information on my rights under PHIA?	**This information is a summary of your rights and our obligations under *PHIA*. There are specific exceptions to these rights and obligations.** Additional information is included in our brochure [*name of custodian's brochure*]. You can also contact our *PHIA* Contact Person at **[contact person's phone number and e-mail address].** For general information on *PHIA*, you can reach the Department of Health and Wellness *PHIA* contact at 1-902-424-5419 or toll-free at 1-855-640-4765. You can also get general information on *PHIA* at www.novascotia.ca/DHW/PHIA or by e-mailing your questions to phia@gov.ns.ca.

Written Privacy Statement	
The Personal Health Information Act	The *Personal Health Information Act* (*PHIA*) came into force in June 2013. This new provincial health information privacy and access legislation is intended to ensure that personal health information management rules in the health sector are clear, consistent and relevant to all records of personal health information, including the electronic health information systems being implemented in Nova Scotia. *PHIA* balances your right to have your privacy protected with the need of the health sector – including our organization – to collect, use and disclose it to provide appropriate care and service to you. As a "custodian" of personal health information under *PHIA,* we have an obligation to protect the privacy of the information we collect, use and disclose about you. This brochure is a summary of the purposes for our management of your personal health information.
What is "personal health information"?	Personal health information is identifying information about you, and includes demographic information (name, address, date of birth), your health card number, information related to your physical and mental health care, and financial information related to your application and eligibility for health care services. Personal health information can be recorded and unrecorded, and continues to be protected after you are deceased.
Why do you collect my personal health information?	We collect it for several purposes: • to inform our decisions related to appropriate health care for you • to disclose to other providers involved in your health care • to ensure that all custodians receive appropriate payment for delivering care (e.g. services that are insured for you through the Department of Health and Wellness) • to conduct research approved under *PHIA* • to plan and manage health care services for you and others in Nova Scotia • for other purposes required or permitted by law
When do you disclose my personal health information to others?	The personal health information we collect from you is used within our organization to provide appropriate care to you. Anyone in our organization who is required to review your personal health information would have access to it. We may disclose it to health professionals outside of our organization if they are in the "circle of care and treatment" for your illness or injury. This information would enable them to provide appropriate care to you.
Do I need to consent to this disclosure?	This disclosure is carried out under the principle of *"knowledgeable implied consent".* This means that we have to provide you sufficient information about the purposes for collecting, using and disclosing your personal health information, and about your right to give or withhold consent. In addition to the information contained in this brochure, you may ask for additional information about the management of your personal health information. If you continue to seek our services, we can assume your consent to our use and disclosure of your personal health information for your health care.
Can I decide who can and can't have access to my personal health information?	You have the right to request that your personal health information not be used or disclosed by a specific health professional or organization. We are required to: • take reasonable steps to comply with your request

	• advise you of any consequences of your request (e.g. one of your health professionals may not be confident that they have sufficient information to provide care to you) • advise anyone to whom your personal health information is disclosed that the information is not complete • advise you that we cannot comply with your request where the information is required by law to collect, use or disclose
How do I request that my personal health information not be used or disclosed?	A form is available from our *PHIA*/Privacy contact person.
Can I request a copy of my personal health information?	Yes – you have the right to request a copy of your personal health information, or request an opportunity to view your personal health information. There are limited exceptions to what you cannot access, including information what was collected during an investigation or information that includes the personal information of another person. We are permitted to charge you a prescribed fee for providing you with a copy of your record or an opportunity to view your record. We can provide you with the fee schedule.
Can I request that something in my personal health information be corrected?	Yes – you may make the request to our *PHIA*/privacy contact person. There are limited exceptions to your right to a correction of your record, including when the information you request to be corrected is part of a professional opinion of a health practitioner.
What happens if you lose my personal health information or someone who isn't authorized to see it gains access to it?	If your personal health information is breached and we believe that this breach may cause you harm or embarrassment, we are required to notify you of the breach. If we don't notify you, we are required to notify the Review Officer for *PHIA.*
Can I make a complaint if I think you have not followed the rules in *PHIA*?	Yes – our organization has a *PHIA* complaints process. Our *PHIA*/privacy contact person can provide you with the necessary information and form.
What if I am not happy with the way your organization has handled my complaint?	You may request a review under *PHIA*. The Review Officer for *PHIA* can be reached at: **Review Officer** ***Personal Health Information Act*** **P.O. Box 181** **Halifax, Nova Scotia B3J 2M4** **Phone: 902-424-4684 Toll-free: 1-866-243-1564 Fax: 902-424-8303**
Who do I contact for more information?	You can reach our *PHIA*/Privacy Contact person at: [custodian's contact person information].

INSERT CUSTODIAN'S
LOGO HERE

April 2014

Retention & Destruction Schedule Template

Original Documents	Guidelines for Retention	Authority for Disposal Necessary	Retention Period (minimum – maximum)	Retention Mode	Disposition Method
Description of each health record category	Indicate the authority for the retention guidelines	Position in the custodian organization responsible for authorizing disposal	Minimum time that the records must be retained by the custodian. Is there a maximum?	Indicate the format on which the record will be held	E.g. cross cut shredding/ wiping hard drive, de-identifying
Financial	Canada Revenue Agency	CFO	7 years	Paper	Cross-cut shredding
Scheduling	?DHW	Executive Director	7 years	Electronic/Paper	cross cut shredding/ wiping hard drive, USB/ physical destruction and discarding of USB, CD, DVD
Care plan/ Assessment	?DHW	Executive Director	7 years	Electronic/Paper	cross cut shredding/ wiping hard drive

Destruction, Disposal & De-identification Checklist

- ☐ The record containing personal health information has been destroyed in appropriate time
- ☐ The destroyed record cannot reasonably be re-constructed
- ☐ Duplicate copies have been destroyed
- ☐ Copies of the record containing personal health information on other sources of media have been destroyed
- ☐ Electronic and wireless media (e.g. CDs, USBs, Hard drives) have been securely destroyed by physically damaging and discarding them, or when the media is to be re-used, it id wiped clean of records
- ☐ Office equipment, such as fax machines, photocopiers, scanners and printers, which have hard drives that retain information are either wiped clean before disposal of the equipment, or the hard drive is disabled
- ☐ Information that is retained past the retention period may be used for the custodian's secondary purposes such as research and quality, as long as it is de-identified. Examples of identifying information is provided below[2]:
    - ☐ Name
    - ☐ Geographic information specific enough to identify individual (e.g. street address, and in some very small regions, postal code??)
    - ☐ Identifying dates excluding the year (e.g. birth date, admission date, discharge date, death date)
    - ☐ Telephone numbers
    - ☐ FAX numbers
    - ☐ Electronic mail addresses
    - ☐ Social Insurance Number
    - ☐ Medical record numbers (health card number??)
    - ☐ Health plan beneficiary numbers/ policy/ id numbers
    - ☐ Account numbers
    - ☐ Certificate/license numbers
    - ☐ Vehicle identifiers and serial numbers, including license plate
    - ☐ Device identifiers and serial numbers
    - ☐ Web universal resource locators (URLs)
    - ☐ Internet protocol (IP) address
    - ☐ Biometric identifiers, including finger and voice prints
    - ☐ Full face photos, and comparable images
    - ☐ Any unique identifying number, characteristic or code (e.g. a revealing occupation, a highly publicized clinical event
    - ☐ Any combination of information, that could be utilized with other information to identify the individual

[2] Based on: Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule (2012).

Substitute Decision-Maker Hierarchy, Selection Criteria and Decision-Making Guide

Hierarchy of Substitute Decision-Makers	Criteria for Choosing a Substitute Decision-Maker	Substitute Decision-Makers Shall Make Decisions Based on the Following
(a) a person who is authorized by or required by law to act on behalf of the individual;	• The potential substitute decision-maker has been in contact with the individual throughout the preceding twelve-month period; or if the individual has not been in contact, a court order has been granted to waive the twelve-month period.	• The prior expressed wishes of the individual. However, the substitute decision-maker may also act according to what s/he believes the individual would have wished had the specific circumstances been known to the individual. In doing this, the substitute decision-maker would base his/her decision on what s/he knows about the values and beliefs of the individual, and any written or oral instructions.
(b) the individual's guardian appointed by a court of competent jurisdiction;		
(c) the spouse of the individual;		
(d) an adult child of the individual;		
(e) a parent of the individual;		
(f) a person who stands in loco parentis to the individual;	• The potential substitute decision-maker is willing to accept the responsibility.	
(g) an adult sibling of the individual;		
(h) a grandparent of the individual;	• The potential substitute decision-maker knows of no person of a higher category who is able and willing to make the decision.	• In the absence of instructions, the substitute decision-maker would base his/her decision on what s/he knows about the values and beliefs of the individual, and any other written or oral instructions.
(i) an adult grandchild of the individual;		
(j) an adult aunt or uncle of the individual;		
(k) an adult niece or nephew of the individual;	• The potential substitute decision-maker certifies in writing the potential substitute decision-maker's relationship to the individual and the facts that meet the criteria set out above.	• Where the substitute decision-maker does not know the wishes, values and beliefs of the individual, the substitute decision-maker may make decisions that s/he believes would be in the best interest of the individual.
(l) any other adult next of kin of the individual;		
(m) the Public Trustee.		

Privacy Complaints Regarding Personal Health Information Policy Template

Policy

Under the Personal Health Information Act, custodians are required to maintain a privacy complaints policy, outlining the process by which individuals making a complaint must follow, and how they can expect their complaint to be dealt with.

An individual can make a complaint regarding a custodian's conduct in relation to privacy provisions under PHIA regarding the following:

- Consent
- Substitute decision makers
- Collection, use disclosure
- Retention, destruction, disposal and de-identification
- Research
- Practices to protect Personal Health Information
- Reporting of a privacy breach

Procedure

How does an individual make a complaint?	An individual with a complaint regarding any of the above provisions under PHIA should contact the custodian's PHIA contact person (see below). **The complainant is required under PHIA regulations to make the complaint in writing**. Complaint forms (attached) should be made available to the complainant. (e.g. directing to website/providing hard copies)
How long do I have to reply to the complaint?	Under PHIA, once the complaint has been received, the custodian must process, investigate, make a decision based on the investigation, and notify the complainant within **60 days**. Complaint response times are as follows: • Within 60 days (Standard) • Within 90 days as long written notice is given to complainant within the first 60 days □ 90+ days, only with the permission of the Review Officer, and if the following apply: o Replying to the complaint within the 30-day extension period would unreasonably interfere with the activities of the custodian o The time required to undertake the consultations necessary to reply to the request within the 30 day extension period would make it not reasonably practical to reply within that time.
How should I handle the investigation of the complaint?	Once a complaint is received, the custodian should follow-up with the complainant to confirm receipt of the complaint and explain how the investigation process will work. The custodian should also determine who else needs to be involved in the investigation. It must be made clear to the individual that their personal health information may need to be accessed and disclosed in order to fully investigate the complaint. The custodian should be a specific as possible, regarding the information involved, and to whom the information may be disclosed, and why. **The individual must provide consent for this.** The individual must also be informed that a full investigation may not be possible if the relevant personal health information is not available to the custodian.

	The custodian investigating should ask the complainant for the following information: o names of all individuals within the custodian's organization who may have information related to the complaint, o all dates relevant to the complaint, o copies of all documents or materials relevant to the complaint, including any previous correspondence between the individual and the custodian, and any background materials relevant to the complaint, o any attempts the individual has made to resolve the complaint, o any harm or embarrassment that has been caused to the individual as a result of the custodian's actions; and o the outcome the individual is seeking from the custodian in relation to the complaint. The custodian should keep track all communications with the complainant, and other involved during the investigation, including, the date and content of the conversation. All information related to the complaint and the investigation of the complaint should be kept separate from the individual's personal health record, so as not to potentially negatively impact their care. Depending on the situation, there may be an opportunity to resolve the complaint informally. If the custodian thinks that the situation can be handled without a full investigation (e.g. further explanation to the individual about their personal health information practices), (s)he should confirm with the complainant whether or not they are feel their issue has been resolved. The date, parties and outcomes of this discussion should be documented. If the individual is not satisfied, the custodian can choose to investigate the complaint further, or can deem the informal resolution as a final decision. However doing so would be considered the completion of the complaints process, thereby allowing the individual to directly proceed to the review officer.
How should I follow-up with the complainant?	Communication with the complainant throughout the process can occur through a variety of media (e.g. phone, email, letters), as per the complainant's preference. However, for outcomes of the investigation and final decisions, a formal written letter must be issued to the complainant, which must include a statement notifying the complainant that they have the right to proceed to the Privacy Review Officer. If the complainant is not satisfied with the resolution, (s)he has the right to contact the Privacy Review Officer, however this cannot be initiated until the internal review process has been completed, and a decision has been rendered. **Note:** The Privacy Review Officer can initiate a review under reasonable grounds. The Privacy Review Officer can also initiate a review if the custodian fails to follow the timelines outlined in this policy, as this would be deemed a refusal to respond to the complaint.
PHIA Contact Person	**Name:** **Position** **Contact Information:**

INSERT CUSTODIAN'S
LOGO HERE

April 2014

Privacy Complaint Form

This form is provided to allow you to provide all information related to your complaint.
You may also send a letter outlining your complaint to the *Personal Health Information Act* contact person for our organization (see below for contact information).

PATIENT/CLIENT/RESIDENT NAME AND CONTACT INFORMATION (please print clearly)

Last Name First Name Middle initial

Mailing address

Daytime telephone number

E-mail address (only required if you wish to be contacted by e-mail)

How do you wish to be contacted? Please check one

- ☐ Phone
- ☐ Regular mail
- ☐ E-mail

If you are making the complaint on behalf of someone else, please provide your name and contact information. You must also attach a copy of the document authorizing you to make the complaint (Example: written consent of the individual, guardianship documents)

Last Name First Name Middle initial

Relationship to patient/client/resident

Mailing address

Daytime telephone number

E-mail address (only required if you wish to be contacted by e-mail)

How do you wish to be contacted? Please check one

- ☐ Phone
- ☐ Regular mail
- ☐ E-mail

DETAILS OF THE COMPLAINT

Please provide as much information as you can about the complaint you are making. Please include details of the incident(s) leading to your complaint, the name of any individuals who are involved in the incident(s), the date when the incident(s) occurred, and any information about your efforts to attempt to resolve this complaint outside of this complaint process (e.g. informal discussions with someone involved in the incident).
Please attach any documents relevant to the complaint.

RESOLVING THE COMPLAINT
What do you think should happen to resolve your complaint?

CONSENT AND SIGNATURE

In order to fully investigate your complaint, we will need to review your personal health information relevant to your complaint. Please check and initial your response.

___ I consent to the [name of custodian] reviewing my personal health information in order to fully investigate my complaint.

___ I **do not** consent to the [name of custodian] reviewing my personal health information in order to fully investigate my complaint.

We may also need to discuss the facts presented on this form and any other information related to the complaint with individuals in our organization**. We would only disclose information relevant to the complaint.**

___ I consent to the [name of custodian] discussing the facts presented on this form and any other information related to the complaint with individuals in [name of custodian]. I understand that [name of custodian] will only disclose information relevant to my complaint.

___ I **do not** consent to the [name of custodian] discussing the facts presented on this form and any other information related to the complaint with individuals in [name of custodian].

Please note that we may not be able to fully investigate your complaint if we do not have access to all the relevant information related to your complaint.

Signature _____

Date _____

Please deliver or mail your original form to:

Name of contact person
Name of custodian
Address of custodian
Phone: 902-XXX-XXXX
Fax: 902-XXX-XXXX

If you have any questions about this form or the process for making a complaint, please contact the [name of contact person, name of custodian].

Privacy Breach Reporting Policy Template

Policy

A **privacy breach** of personal health information is the intentional or unintentional unauthorized access, use, disclosure, copying or modification of personal health information.

A privacy breach policy is not required by PHIA, however it is prudent for custodians to have policies and procedures in place to follow, should a policy breach occur.

Under PHIA a custodian is required to notify the breach subject at the "first reasonable opportunity" if it is reasonable to believe that:

- the information is stolen, lost or subject to unauthorized access, use, disclosure, copying or modification; **AND**
- as a result, there is potential for harm or embarrassment to the individual

Procedure

After a potential breach has been discovered:

1. Notify Internally	The person who uncovers the potential breach should notify the custodian's Privacy Contact Person, their immediate supervisor, and depending on the situation, custodian's CEO, Board and legal counsel.
2. Contain	Once a privacy breach is discovered, every effort should be made to contain the breach to ensure the personal health information is not breached further (e.g. if a fax or email containing personal health information is sent to the wrong address, the unintended recipients of the information and followed up with and asked to destroy the information and provide confirmation of doing so).
3. Investigate	The investigation process includes a determination of the 2 factors required for a privacy breach to have occurred. - the information is stolen, lost or subject to unauthorized access, use, disclosure, copying or modification; **AND** - as a result, there is potential for harm or embarrassment to the individual. Scope of Harms ▪ Physical harm(s) ▪ Psychological harm(s) including embarrassment, humiliation and threat to dignity ▪ Financial/economic burdens ▪ Identity theft and/or fraud ▪ Reputational harm (damage to the breach subject's reputation) ▪ Basis(es) for potential discriminatory action(s) that may be taken against the breach subject ▪ Social/relational harm (damage to the breach subject's relationships)

The investigation should also consider factors that favor and do not favor notification

Factors that favor notification of the breach subject or SDM	Factors that do not favor notification of the breach subject or SDM
The breach subject(s) and the individual(s) who breached the information are known (e.g., personally or vocationally connected) to each other.	The recipient of the breached information is an individual or office where the individual/staff is bound by the confidentiality obligations of a regulated profession.
The breached information directly connects/links the breach subject's name with her/his medical diagnosis(es).	There was no or minimal opportunity to access the breached information.
There are multiple recipients (e.g., individuals and/or offices) of the breached information.	The initial response to identification and containment of the privacy breach was appropriate, timely and effective.
The individual who breached the personal health information of the breach subject breached the information of another/others.	
The personal health information of the breach subject was breached more than once.	
The breach has led, or could potentially lead, to other/further breaches of personal health information.	

4. Notify Externally

If the investigation determines that neither of the required factors for a privacy breach have occurred, the subject of the breach does not need to be notified. However, in this situation the Review Officer must be notified of the incident, including the details and results of the investigation, using the **Privacy Breach Reporting Form (attached)**.

If the investigation determines that both factors are present and that a privacy breach has occurred, the breach subject must be notified as soon as reasonably possible. **The subject of the breach should not be notified until a full investigation of the breach has occurred.**

Notification to the breach subject(s) or SDM(s) should include:

- The date(s) the privacy breach occurred
- The date the breach was discovered
- A description of the personal health information that was breached
- A description of the actions the custodian is taking to investigate, minimize harms to the breach subject(s), and prevent further privacy breaches
- The custodian's contact information

	▪ Information regarding the breach subject(s) option to directly contact the Review Officer ▪ As appropriate and available, offer to refer the breach subject to a psychological support provider within the community <u>Notification of the Review Officer should include</u>: ▪ The date(s) the privacy breach occurred ▪ The date the breach was discovered ▪ Brief descriptions of: o The type of information that was breached (not including information that could potentially identify the breach subject(s)) o The privacy breach circumstances o The criteria/factors relied on to make the decision to not notify the breach subject/SDM For further guidance on privacy notification, see the **Privacy Breach Notification Decision Making Tool.**
5. Follow up & Document	The incident should be reviewed to determine if there are precautions that can be taken to ensure a similar breach does not happen again. Further, the incident and details of the investigation should be documented.

INSERT CUSTODIAN'S
LOGO HERE April 2014

Personal Health Information Breach Reporting Form

Please complete this document and provide the completed and signed document to [*Contact Person, Name of Custodian*].

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

Reporting

Date and time of breach

Date and time of breach was reported

Name and position of person(s) who reported the breach

Details of breach (include name(s) and contact information for all individuals whose information was allegedly breached)

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.

Investigation of the breach

Determination of whether notification of the breach subject is required.

- the information is stolen, lost or subject to unauthorized access, use, disclosure, copying or modification; **AND**
- as a result, there is potential for harm or embarrassment to the individual.

Other factors to consider (see **Privacy Breach Notification Tool** for further explanation of these).

Factor	Comment
Type of information breached and degree of sensitivity	
Scope of breach (# subjects and recipients of breach, length of time, # of breaches)	
Method (e.g. hacking/theft vs. incorrect email/fax)	
Recipient(s) (e.g. agent vs. media/public)	
Intent (accidental vs. malicious)	
Disposition (returned/destroyed vs. further breached/unable to retrieve)	
Safeguards (none vs. encryption)	
Anticipated impact of notification (human, financial resources)	

Scope of Harms (check all that apply)

- ☐ Physical harm(s)
- ☐ Psychological harm(s) including embarrassment, humiliation and threat to dignity
- ☐ Financial/economic burdens
- ☐ Identity theft and/or fraud
- ☐ Reputational harm (damage to the breach subject's reputation)
- ☐ Basis(es) for potential discriminatory action(s) that may be taken against the breach subject
- ☐ Social/relational harm (damage to the breach subject's relationships)

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.

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

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.**

Signatures & Date

Reporting breach _____
Privacy Contact Person_____

Notes from Contact Person

Include any additional relevant information (e.g. details of any complaint lodged by the individuals, a request from the individual or the custodian to the Review Officer to investigate).

Personal Health Information Safeguards

Administrative Safeguards	**Physical Safeguards**	**Technical Safeguards**
Appointment of a privacy officer/*PHIA* contact person (*PHIA* section 67*)*	Establishing secure areas and using identity badges in secure areas (where required and feasible).	**Measures to protect network infrastructure** E.g. protection against unauthorized access to protect network infrastructure from external (e.g. malware and hackers) and internal threats (e.g. network operational centres should be kept locked).
	Maintaining access records for individuals who have access to secure areas. The access records should be meaningful in the event of a security audit.	
Written security policies/guidelines (*PHIA* regulation section 10(2))	Ensuring that appropriate security mechanisms are used at any unattended entrance to a secure area (e.g. locks on doors, card access control, monitored surveillance cameras).	**Measures to protect hardware/operating systems** For example, back-up information should be stored in a secure, locked environment off-site. Information intended for long-term storage on electronic media should be reviewed on a regular basis to ensure the data is retrievable, and to migrate the data to another storage medium if necessary.
	Placing monitors, printers and fax machines where others cannot see personal health information (e.g. away from waiting rooms, ground floor windows or busy passageways).	
Written privacy statement (*PHIA* section 15*)* [2]	Ensuring equipment is kept in a locked office whenever you are out of the office or away for extended periods of time (e.g. overnight, vacation).	**Measures to protect a system's software and data** • Disaster recovery models by having up-to-date backups of all data securely stored in a separate location. • Encryption and authentication minimizes the risk of access by unauthorized individuals. Encryption/cryptography are mechanisms to convert data for secure transmission or storage. Authentication is any process that verifies the source of a request or response for information in a computing environment. Authentication can be based on one or more of the following criteria: 1. something you have – e.g. a key, card 2. something you know – e.g. password, personal I.D. number 3. something related to who you are – e.g. signature, iris pattern, voiceprint, thumb print 4. something indicating where you are located – e.g. terminal
Staff privacy and confidentiality training to maintain awareness of policies and guidelines	Ensuring equipment is kept in a locked office whenever you are out of the office or away for extended periods of time (e.g. overnight, vacation).	
	Keeping portable equipment secure (e.g. do not leave laptops in your vehicle).	
Audits (including an audit schedule) for compliance with security policies	Keeping USB memory devices, CDs, and other media in a secure place (e.g. a locked drawer).	
	Maintaining the ability to quickly restore critical systems in the event of equipment loss or failure.	
Contracts with agents that ensure compliance with the	Disposing of all media containing sensitive information in a secure manner, which includes shredding, disintegration and incineration	

Act and regulations	Establishing secure areas and using identity badges in secure areas (where required and feasible).	connected by hardwired line, phone number • Antivirus/antimalware can protect against unauthorized modification, loss, access, or disclosure. As viruses and malware threats are constantly changing and advancing, it is important to ensure antivirus/antimalware software is up-to-date to protect from such threats. • Internet access should be through a firewall implemented through hardware (e.g. network router) or software residing on the user machine. • Particular attention is required to protect data during transport or on a mobile device. There are different considerations that should be taken into account to ensure the security of the data. ○ Devices such as laptops, memory sticks and smart phones may facilitate mobility; however these devices should only be utilized for personal health information if the appropriate security measures are in place. ○ Encryption may mitigate the risk of transporting data and it is recommended that, when taking data from a secure office location and putting it onto a mobile device or transporting it otherwise, data should be encrypted. Security is also dependent on the person not sharing their access directly or indirectly, through careless storage of user IDs and passwords. Another element of security is restricting access to personal health information by staff on a need-to-know basis; only those who need to have access to the personal health information for the purpose of carrying out their job functions should have access.
Confidentiality agreements for employees and agents	Maintaining access records for individuals who have access to secure areas. The access records should be meaningful in the event of a security audit.	
	Ensuring that appropriate security mechanisms are used at any unattended entrance to a secure area (e.g. locks on doors, card access control, monitored surveillance cameras).	
	Placing monitors, printers and fax machines where others cannot see personal health information (e.g. away from waiting rooms, ground floor windows or busy passageways).	
	Keeping portable equipment secure (e.g. do not leave laptops in your vehicle).	
	Keeping USB memory devices, CDs, and other media in a secure place (e.g. a locked drawer).	
	Maintaining the ability to quickly restore critical systems in the event of equipment loss or failure.	
	Disposing of all media containing sensitive information in a secure manner, which includes shredding, disintegration and incineration.	
	Taking appropriate measures while in transit to personal health information of clients.	

Requests for Access to Personal Health Information Policy Template

Policy

Requests

Under *PHIA* an individual has the right to access a record of their personal health information. In order for an individual to request access to their personal health information:

- The request must be made in writing to the custodian of the personal health information (a **request form is attached**).
- The request for access must specify the subject matter of the record requested with sufficient information to enable the custodian to locate the record.
- The individual must pay any required fees (unless waived by custodian).
- **The individual does not have to provide the reasons or purposes for which they are requesting the information**.

Fees

A custodian has the right to charge a fee for access to personal health information where the fee does not exceed the prescribed amount, or where no amount is prescribed, the amount of "reasonable cost recovery". A custodian must first provide a fee estimate to the individual, although the final fee payable may be altered if the actual costs to the custodian were higher (see **attached fee schedule**). **The fee should not be a barrier to access.** The custodian has the discretion to waive all or part of an access fee, if the custodian feels the individual cannot afford the fee, or for any other reason it would be fair to excuse payment (**request for fee waiver attached**). If a custodian receives a request to waive the fee, there may be opportunities to narrow the request, thereby decreasing the fee. While the custodian is not obligated to reduce or waive the fee, a complaint can be made to the Review Officer, and so it would be prudent for the custodian to document the reasons for refusal.

Refusal

There are several exceptions, whereby a custodian can refuse to grant access in full, or partially to the individual's personal health information, outlined below. Where it is reasonable to believe that:

- A legal privilege restricts disclosure.
- Another law prohibiting disclosure.
- The information in the record was collected or created primarily for the purpose of ensuring quality or standards of care within a quality review program in the custodian's organization.
- The information in the record was collected or created in anticipation for use in a proceeding, or in the course of an inspection, investigation or similar procedure, not yet concluded.
- Access could result in a risk of serious harm to the treatment or recovery of the individual or to the mental or physical health of the individual, or another individual.
- Access could lead to the release of another individual's personal health information, or to the identification of a person who provided information in the record to the custodian in circumstances where confidentiality was reasonably expected.
- The request for access is either frivolous or vexatious, suggesting a pattern of abuse of right of access.

If a request is refused, the custodian must notify the individual in writing, justifying why the request was refused, and also inform the individual that (s)he has the right to make a complaint to the Review Officer

Procedure

Once a written request for personal health information is received:

Respond	A custodian who receives a request for access must respond, in writing, as soon as possible; **no later than 30 days** after receiving the request. In the written response, the custodian must grant the request, refuse the request, or extend the deadline. **A Response Form is attached.**
a. Grant request	If the request is granted, the custodian must notify the individual in writing. The custodian is also required to provide a fee estimate for accessing the information. Although PHIA does not require a fee estimate to be given in writing, an **Estimate of Fees Form is attached.**
b. Refuse request, in part or in full	When denying access to all or part of an individual's personal health information on reasonable grounds, the onus is on the custodian to justify their decision. The custodian must: • Give written notice to the individual, outlining the reasons for refusal • State that the individual has the right to make a compliant to the Review Officer
c. Extend deadline to reply	A custodian can extend the deadline to respond the request by up to 30 days. An extension of greater than 30 days requires permission by the Review Officer. Extensions for replying to the request may only be applied where doing so within 30 days would unreasonably interfere with the activities of the custodian, or if the time required to complete the necessary consultations would not make it reasonable to do so. The written notice should state the length, and reasons for the extension.

INSERT CUSTODIAN'S
LOGO HERE

April 2014

REQUEST FOR ACCESS TO PERSONAL HEALTH INFORMATION

1. IDENTIFICATION OF INDIVIDUAL (please print clearly)

Last Name	First Name	Middle initial
Previous surname (if applicable)		Date of birth (YY/MM/DD)
Provincial Health Card Number		Daytime telephone number
Mailing address		

2. IDENTIFICATION OF RECORDS

Please indicate which records you are seeking to access:

Please indicate what portion of the record(s) you are seeking to access:

- ☐ The whole record
- ☐ All records from the time period _____ to _____
  (yyyy/mm/dd) (yyyy/mm/dd)
- ☐ The following specific records: _____

3. TERMS OF ACCESS

I wish to access the records as follows:

- ☐ View only
- ☐ Photocopies

If receiving photocopies of the records, I wish to:

- ☐ have the records delivered to me by regular mail
- ☐ have the records delivered to me by courier
- ☐ pick the records up in person

4. SIGNATURE

I consent to the **[name of custodian]** reviewing my personal health information in order to provide it to me as requested on this form. I understand that there may be a fee for access to my records, including any fee associated with delivery by regular mail or courier. The **[name of custodian]** must provide an estimate of any fees to me prior to release of my record(s), and fees may be payable by me in advance of any access.

Signature	**Date**

Please deliver or mail your form to:
Name of contact person
Name of custodian
Address of custodian
Phone: 902-XXX-XXXX Fax: 902-XXX-XXXX

The personal health information requested in this form is collected pursuant to s. 75 of the *Personal Health Information Act* for the purposes of processing your request for access to your information. If you have any questions about this form or the process for requesting access, please contact [name of contact person, name of custodian].

INSERT CUSTODIAN'S
LOGO HERE April 2014

ESTIMATE OF FEES – ACCESS TO PERSONAL HEALTH INFORMATION

[Date]

This form is used to state the estimate of fees payable under section 82 of the *Personal Health Information Act (PHIA)* for access to your personal health information. **Please note that this is an estimate only**. The actual fees may be lower or higher, but will not exceed the amount prescribed in the *Personal Health Information Act* Regulation. Please direct any questions about this fee estimate to the contact listed below.

The estimate of fees for access to your record is:

General Fee (maximum $30.00)	_____
Specific fees (see attached for detail)	_____
Direct costs	_____
HST	_____
Total estimate of fees	**_____**

Please acknowledge your acceptance of the above estimate by signing below and returning the **original** of this form to our office. In order to process your request for access, we require [ ] of the above fees.

I, _____ *(print name)* accept the fee estimate as stated on this form. I understand that the actual fee may be higher, but will not exceed the amount prescribed in the *Personal Health Information Act* Regulations.

_____ _____
Signature Date

Please deliver or mail your original form to:
Name of contact person
Name of custodian
Address of custodian
Phone: 902-XXX-XXXX
Fax: 902-XXX-XXXX

You have the right to request a review of this fee estimate decision by the Review Officer appointed pursuant to *PHIA.* The review must be filed with the Review Officer in writing within 60 days of the date of this letter. The **Request for Review Form** is attached. The form should be sent to:

Review Officer
Personal Health Information Act
P.O. Box 181
Halifax, Nova Scotia, B3J 2M4
Phone: 902-424-4684 Toll-free: 1-866-243-1564 Fax: 902-424-8303

Detail of Fee Estimate

1. General fee

The activities charged under the **General Fee** include:

- receiving and clarifying the request;
- locating and retrieving the record (including records held electronically);
- providing an estimate of the access fee to the requester;
- review of the record for not more than 15 minutes by a health information custodian or an agent of the custodian to determine if the record contains personal health information to which access may be refused under *PHIA* s. 72(1);
- severing of the record where access may be refused under *PHIA* s. 72(1);
- preparation of the record for photocopying, printing or electronic transmission for not more than 30 minutes;
- preparation of a response letter to the requester;
- supervising an individual's examination of original records for not more than 30 minutes; and
- the cost of mailing a record by regular mail to an address in Canada.

2. Specific Fees

In accordance with the *Personal Health Information Act* Regulation, additional specific fees may be charged in addition to the general fee, and any direct costs (see below). For your request, the maximum additional specific fees are:

- photocopies (@ $.20/page)
- preparation of the record (@ $12.00 for every 30 minutes after the first 30 minutes referenced in the general fee)
- faxing a record (@ $.20/page)
- Making a:
    - CD of the record (@$10.00 per request)
    - microfiche copy of microfiche (@ $.50/page)
    - paper copy of microfiche (@ $.50/page)
    - copy of audio cassette (@$5.00 per cassette)
    - copy of video cassette (1 hour or less = $18.00; more than 1 hour = $23.00)
- producing a copy of medical film (@$5.00 per film)
- printing a photograph (@$10.00-$32.00 per print, depending on size)
- review for severing (over 15 minutes) (@$25.00 for every 15 minutes past the first 15 minutes)
- supervision of your examination of your record ($6.00 for every 30 minutes past the first 30 minutes)

3. Direct fees

In accordance with the *Personal Health Information Act* Regulation, direct cost fees may be charged in addition to the general fee and any specific fees. For your request, the direct costs are:

- individual's request for expedited access and retrieval
- individual's request for delivery by courier
- individual's request for mailing to an address outside Canada
- taxes payable on the services provided

INSERT CUSTODIAN'S
LOGO HERE

April 2014

Request for Fee Waiver – Access to Personal Health Information

[Date]

This form is used to request a reduction or waiver of the fee estimated by [name of custodian] to provide access to personal health information.

The *Personal Health Information Act* section 82(3) provides that a custodian has the discretion to determine whether to grant a fee waiver request if, in the custodian's opinion, the individual cannot afford the payment or for any other reason it is fair to excuse payment.

Please attach a copy of the fee estimate provided by _____ or state below the fee amount estimated by _____ to fulfill your access request. You may attach other documents to support your request.

I am requesting a fee reduction/waiver of the following fee(s):

Reasons for request:

Signature Date

Please deliver or mail your original form to:
Name of contact person
Name of custodian
Address of custodian
Phone: 902-XXX-XXXX
Fax: 902-XXX-XXX

INSERT CUSTODIAN'S
LOGO HERE April 2014

RESPONSE TO REQUEST FOR ACCESS TO PERSONAL HEALTH INFORMATION

[Date]

I am writing in response to your request under the *Personal Health Information Act* for the following records:

[restate information from individual request]

Your request has been:

- ☐ granted in full
- ☐ granted in part
- ☐ denied

For requests granted in part or denied only:
Information has been severed/ denied access pursuant to section 72(1) of *PHIA*

- ☐ A legal privilege restricts disclosure.
- ☐ Another law prohibits disclosure.
- ☐ The information in the record was collected or created primarily for the purpose of ensuring quality or standards of care within a quality review program in the custodian's organization.
- ☐ The information in the record was collected or created in anticipation for use in a proceeding, or in the course of an inspection, investigation or similar procedure, not yet concluded.
- ☐ Access could result in a risk of serious harm to the treatment or recovery of the individual or to the mental or physical health of the individual, or another individual.
- ☐ Access could lead to the release of another individual's personal health information, or to the identification of a person who provided information in the record to the custodian in circumstances where confidentiality was reasonably expected.
- ☐ The request for access is either frivolous or vexatious, suggesting a pattern of abuse of right of access (section 81(1)).

Further Comments:

You have the right to request a review of this decision by the Review Officer appointed pursuant to *PHIA.* The review must be filed with the Review Officer in writing within **60 days** of the date of this decision letter. The attached **Request for Review Form**, should be sent to:

Review Officer
Personal Health Information Act
P.O. Box 181
Halifax, Nova Scotia
B3J 2M4
Phone: 902-424-4684 Toll-free: 1-866-243-1564 Fax: 902-424-8303

If you have any questions related to this response, you may contact:
Name of contact person
Name of custodian
Address of custodian
Phone: 902-XXX-XXXX Fax: 902-XXX-XXXX

Requests for Correction of Personal Health Information Policy Template

Policy

Under PHIA an individual may request that a custodian corrects information contained within their records of personal health information. **A fee cannot be charged for this**.

The custodian is not required to correct a record if:

- It consists of a record that was not originally created by the custodian and the custodian does not have sufficient knowledge, expertise, and authority to correct the record.
- It consists of a professional opinion or observation that a custodian has made in good faith about the individual (section 87(2)).
- A custodian may also refuse to correct a record where the custodian believes on reasonable grounds that the request for correction is frivolous or vexatious or suggests a pattern of conduct that amount to abuse of the right to correction.

Procedure

Once a request for correction to personal health information is received (see form):

Respond	A custodian who receives a request for correction must respond, in writing, as soon as possible, **no later than 30 days** after receiving the request. In the written response, the custodian must grant the request, refuse the request, or extend the deadline. **A Response Form is attached***
a. Grant request	If the request is granted, the custodian must notify the individual in writing.
b. Refuse request, in part or in full	If the custodian refuses to make the correction the custodian must give the reasons for the refusal and inform the individual that the individual is entitled to: • prepare a concise statement of disagreement setting out the correction the custodian refused to make; • require that the custodian attach the statement of disagreement as part of the records; • disclose the statement of disagreement whenever the custodian discloses information to which the statement relates; • require that the custodian make all reasonable efforts to disclose the statement of disagreement to any person who would have been notified had the request been granted; and • make a complaint about the refusal to the Review Officer.
c. Extend deadline to reply	A custodian can extend the deadline to respond the request by up to 30 days. An extension of greater than 30 days requires permission by the Review Officer. Extensions for replying to the request may only be applied where doing so within 30 days would unreasonably interfere with the activities of the custodian, or if the time required to complete the necessary consultations would not make it reasonable to do so. The written notice should state the length, and reasons for the extension.
Correcting Information	If a correction is made, the custodian should: • Record the correct information in the record and strike out the incorrect information without obliterating the record.

	• Where it is not possible to correct the information in this manner, a custodian may make the correction by: labeling the information as incorrect; severing the incorrect information from the record; storing it separately from the record; and maintaining a link in the record that indicates that a correction has been made and enables the tracing of the incorrect information. • If a custodian cannot correct a record by either of these two methods, the custodian must ensure that there is a practical system in place to inform a person who accesses the record that the information in the record is incorrect and direct the person to the correct information.
Follow-up	The custodian must provide written notice to the individual about how the record was corrected. On the request of the client, the custodian must also make a reasonable effort to give written notice of the correction to the persons to whom the custodian has disclosed the information, unless the correction cannot be reasonably expected to have an effect on the ongoing provision of health care or other benefits to the patient.

INSERT CUSTODIAN'S
LOGO HERE

April 2014

REQUEST FOR CORRECTION TO PERSONAL HEALTH INFORMATION

1. IDENTIFICATION OF INDIVIDUAL (please print clearly) [DATE]

Last Name First Name Middle initial

Previous surname (if applicable) Date of birth (YY/MM/DD)

Provincial Health Card Number

Mailing address

Daytime telephone number

2. REQUEST FOR CORRECTION

Please provide a detailed description of the personal health information you are seeking to correct. Please be as specific as possible, including the date of the record, the reason for seeking the correction (e.g. the information is not accurate, complete or up-to-date), and the specific correction(s) you are seeking. If possible, please attach the relevant portion of the specific record.

3. SIGNATURE

I consent to ***[name of custodian]*** reviewing my request for correction and the personal health information I am seeking to correct.

Signature **Date**

Please deliver or mail your form to:
Name of contact person
Name of custodian
Address of custodian
Phone: 902-XXX-XXXX
Fax: 902-XXX-XXXX

The right to request a correction to your personal health information is pursuant to ss. 85 - 90 of the *Personal Health Information Act.* A custodian is not required to correct the information if:

a. it consists of a record that was not originally created by ***[name of custodian]*** and ***[name of custodian]*** does not have sufficient knowledge, expertise and authority to correct the record;
b. it consists of a professional opinion or observation that a custodian has made in good faith about an individual;
c. the ***[name of custodian]*** believes on reasonable grounds that a request for a correction
    i) is frivolous or vexatious; or
    ii) is part of a pattern of conduct that amounts to an abuse of the right of correction.

If ***[name of custodian]*** does not correct the information for the reason(s) listed above, written notice will be provided to you.

If you have any questions about this form or the process for requesting a correction, please contact [name of contact person, name of custodian].

INSERT CUSTODIAN'S
LOGO HERE April 2014

RESPONSE TO REQUEST FOR CORRECTION TO PERSONAL HEALTH INFORMATION

[Date]

Dear [*insert individual's name*]:

I am writing in response to your request under the *Personal Health Information Act (PHIA)* for the following correction to your personal health information:

[restate information from individual's request]

Your request has been:

- ☐ granted in full
- ☐ granted in part
- ☐ denied

For requests granted in full or granted in part

Pursuant to s. 88(a) of *PHIA,* your personal health information has been corrected as follows:

[State how the correction has been made.] Options are:

1. *The information has been struck out without obliterating the record.*
2. *Where that is not possible:*
    a. *the information has been labeled as incorrect;*
    b. *the incorrect information has been severed from the record;*
    c. *the incorrect information has been stored separately from the record; and*
    d. *a link has been maintained in the record that indicates that a correction has been made and enables a person to trace the incorrect information.*
3. *Where it is not possible to record the correct information in the record, we have ensured that there is a practical system in place to inform a person who accesses the record that the information in the record is incorrect and to direct the person to the correct information [explain the process put in place].*

For requests granted in part or denied

The reason for not granting (the remainder) of your request for correction is as follows:

[State the reason for the refusal. The options are:

a) *The information was not originally created by me/us, and I/we do not have sufficient knowledge, expertise and authority to correct the record; or*

b) *The information is a professional opinion or observation that I/we have made in good faith about you; or*

c) The request is frivolous or vexatious or suggests a pattern of conduct that amount to abuse of the right to correction.

Pursuant to s. 90 of *PHIA*, for the portion of your request which was not granted, you are entitled to:

a) prepare a concise statement of disagreement that sets out the correction that I/we have refused to make;

b) require that the I/we attach the statement of disagreement as part of the records I/we hold of your personal health information;

c) disclose the statement of disagreement whenever the I/we disclose information to which the statement relates;

d) require that the I/we make all reasonable efforts to disclose the statement of disagreement to any person who would have been notified under clause 88(c) of the *Personal Health Information Act* [see below] if I/we had granted the requested correction; and

e) make a complaint about the refusal to the Review Officer.

Section 88(c) of *PHIA* states that when a request for correction is granted, I/we shall, at your request*, "give written notice of the requested correction, to the extent reasonably possible, to the persons to whom the custodian has disclosed the information unless the correction cannot reasonably be expected to have an effect on the ongoing provision of health care or other benefits to the individual."*

If you choose to prepare a statement of disagreement, or if you have any questions related to this response, you may contact:
Name of contact person
Name of custodian
Address of custodian
Phone: 902-XXX-XXXX
Fax: 902-XXX-XXXX

If you are not satisfied with this response, you have the right to request a review of this decision by the Review Officer appointed pursuant to *PHIA.* The review must be filed with the Review Officer in writing within 60 days of the date of this decision letter. The **Request for Review Form** is attached. The form should be sent to:

Review Officer
Personal Health Information Act
P.O. Box 181
Halifax, Nova Scotia
B3J 2M4
Phone: 902-424-4684
Toll-free 1-866-243-1564
Fax: 902-424-8303

Circumstances Under Which Indirect Collection of Personal Health Information is Permissible

- The individual authorizes collection from another person.
- The collection is from the substitute decision-maker if the substitute decision-maker has the authority to act.
- The information to be collected is reasonably necessary for providing health care or assisting in the provision of health care to the individual and it is not reasonably possible to collect, directly from the individual:
    - personal health information that can reasonably be relied on as accurate, or
    - personal health information in a timely manner;
    - the custodian believes, on reasonable grounds, that collection from the individual who is the subject of the information would prejudice the safety of any individual; or
    - for the purpose of assembling a history of family-health issues potentially relating to or also affecting the individual.
- Collection is for:
    - determining the eligibility of an individual to participate in a program of, or to receive a benefit, product or health service from, a custodian, and the information is collected in the course of processing an application made by or for the individual who is the subject of the information, or
    - verifying the eligibility of an individual who is participating in a program of, or receiving a benefit, product or health service from, a custodian to participate in the program or to receive the benefit, product or service.
- The custodian is a public body within the meaning of the *Freedom of Information and Protection of Privacy Act* or is acting as part of such a public body, and the custodian is collecting the information for a purpose related to:
    - investigating a breach of an agreement or a contravention or an alleged contravention of the laws of the Province or Canada;
    - the conduct of a proceeding or a possible proceeding; or
    - the statutory function of the custodian.
- The custodian collects the information from a person who is not a custodian for the purpose of carrying out a research project that has been approved by the research ethics board or a research ethics body, except if the person is prohibited by law from disclosing the information to the custodian.
- The custodian is a prescribed entity mentioned in clause 38(1)(j) and the custodian is collecting personal health information from a person who is not a custodian for the purpose of that clause.
- The custodian collects the information from a person who is permitted or required by law or by a treaty, agreement, or arrangement made under this *Act* or another *Act* of the Province or of the Parliament of Canada to disclose it to the custodian.
- Subject to the requirements and restrictions, if any, that are prescribed, the custodian is permitted or required by law or by a treaty, agreement, or arrangement made under this *Act* or another *Act* of the Province or of the Parliament of Canada to collect the information indirectly.
- The custodian is the Minister of Health and Wellness and the collection of the personal health information is for the purpose of planning and management of the health system.
- The collection is for the purpose of ensuring quality or standards of care within a quality review program within the custodian's organization.
- The collection is reasonably necessary for the administration of payments in connection with the provision of health care to the individual or for contractual or legal requirements in that connection.
- The custodian is the Minister of Health and Wellness and the collection of personal health information is from another custodian for the purpose of creating or maintaining an electronic health record.

Disclosure of Personal Health Information Without Consent Reporting Form

Please provide a description or copy of the personal health information disclosed.

Please provide the name of the person or organization to whom the personal health information was disclosed.

Date of the disclosure:

Why was this information disclosed without consent (e.g. treaty/agreement, provision under an Act)? Note: this does not apply to disclosure of personal health information within the circle of care.

INSERT CUSTODIAN'S
LOGO HERE

April 2014

Limiting/Revoking Consent Request Form

Name:

Please indicate the provider to whom you do not want your personal health information disclosed:

Please indicate the specific personal health information you do not want disclosed to the aforementioned person (please be as specific as possible):

By signing this:

I understand that [custodian] is required to notify the identified individual that my personal health record is incomplete.

I understand that the identified individual may not feel confident in providing care to me without a complete record.

I understand that [custodian] will take all reasonable steps to comply with my request to limit or revoke consent, however there may be circumstances where this is not possible (e.g. due to electronic capabilities).

I understand that this does not apply retroactively, meaning previous personal health information disclosed to the identified individual will not be returned.

I understand that in order to perform my request that [custodian] will have to access the personal health information I am seeking to limit.

Signature **Date**

Please deliver or mail your form to:
Name of contact person
Name of custodian
Address of custodian
Phone: 902-XXX-XXXX
Fax: 902-XXX-XXXX

Limiting/Revoking Consent Response Letter Template

Dear _____,

Your request to limit/revoke consent of [*specific personal health information*] being shared with [*identified individual*] has been received and processed.

Your request has been:

- ☐ granted
- ☐ denied
- ☐ unable to perform request

For granted requests:
The specific information you requested has been [*provide brief explanation of how the information has been made unavailable to the identified individual*]. As per your signed request form, this does not apply retroactively, meaning previous personal health information disclosed to the identified individual will not be returned. The identified individual has been notified that the personal health record they received is incomplete. As indicated in your signed request form, it is under the discretion of [identified individual] if they feel confident providing you care with an incomplete record.

For denied requests:

Your request to revoke/limit consent for [specific information] to be shared with [identified individual] has been denied. We are denying your request under [cite Act] which requires [custodian or identified individual] to collect, use or disclose your [specific personal health information] by law.

For requests unable to be performed:

Your request to revoke/limit consent for [specific information] to be shared with [identified individual] is not able to be performed at this time. We are unable to perform this request because [provide explanation - e.g. our electronic system does not allow us to withhold information] while we are not able to perform this request, you can be assured that only persons involved in your care will have this information disclosed to them.

If you have any further questions regarding your request, please contact [*name and contact information of privacy contact person*].

If you are not satisfied with this response, you may contact the Review Officer:
Review Officer
Personal Health Information Act
P.O. Box 181
Halifax, Nova Scotia
B3J 2M4
Phone: 902-424-4684 Toll-free 1-866-243-1564 Fax: 902-424-8303

RESEARCH PLAN CHECKLIST

Section 59 of the *Personal Health Information Act (PHIA)* requires a researcher seeking to conduct research utilizing personal health information to submit a research plan to a Research Ethics Board[i]. The research plan must be in writing, and in order to meet the requirements for a custodian under the *Act*, the research plan must include the following:

- a description of the research[ii] proposed to be conducted;
- a statement regarding the duration of the research;
- a description of the personal health information required and the potential sources of the information;
- a description as to how the personal health information will be used in the research;
- where the information will be linked to other information, a description of the other information as well as how the linkage will be conducted;
- where the researcher is conducting the research on behalf of or with the support of a person or organization, the name of the person or organization;
- the nature and objectives of the research and the public or scientific benefit anticipated as the result of the research;
- where consent is not being sought, an explanation as to why seeking consent is impracticable;
- an explanation as to why the research cannot reasonably be accomplished without the use of personal health information;
- where there is to be data matching[iii], an explanation of why data matching is required;
- a description of the reasonably foreseeable risks arising from the use of personal health information and how those risks are to be mitigated;
- a statement that the personal health information is to be used in the most de-identified form possible for the conduct of the research;
- a description of all individuals who will have access to the information, and:
    - why their access is necessary;
    - their role in relation to the research; and
    - their qualifications;
- a description of the safeguards that the researcher will impose to protect the confidentiality and security of the personal health information;
- information as to how and when the personal health information will be destroyed or returned to the custodian;
- the funding source of the research;
- whether the researcher has applied for the approval from another research ethics board and, if so, the response to or status of the application; and
- whether the researcher's interest in the disclosure of the personal health information or the conduct of the research would potentially result in an actual or perceived conflict of interest on the part of the researcher.

NOTIFICATION TO REVIEW OFFICER

Research – *Personal Health Information Act* section 57(d)

(Date)
Review Officer
Personal Health Information Act
Box 181
Halifax, NS
B3J 2M4

Dear [name of Review Officer]:

Please accept this letter as notification that [name of custodian] has approved the attached research plan from [name of researcher].

The [name of researcher] has met the requirements of the *Personal Health Information Act* to the satisfaction of [name of custodian] which includes use or disclosure of personal health information without consent of the subject individuals.

Sincerely,

(signature)
Custodian

DATA DISCLOSURE AGREEMENT FOR RESEARCH PURPOSES

NOTE TO USER: This Sample Data Release Agreement is intended to be used for retrospective research when a custodian discloses personal health information to an external researcher. It would not be used when a researcher who is an agent of the custodian (e.g. an employee of the custodian uses personal health information collected by the same custodian).

I. PARTIES

This Agreement is made between (*insert name of Custodian) hereinafter known as "the Custodian"* and (*insert name of Researcher*) hereinafter known as "the Researcher".

II. GENERAL

The *Personal Health Information Act* (*PHIA*) allows for the use and disclosure of personal health information for research purposes, but places strict guidelines on the release of this information.

III. BACKGROUND

(a) (*identify Custodian*)
(b) (*identify Researcher)*
(c) Outline the details of the proposed disclosure of personal health information and the Research Plan

IV. PURPOSE

The purpose of this document is to set out terms and conditions about the collection, use, disclosure, retention, disposal and destruction of personal health information provided by the Custodian to the Researcher.

V. INFORMATION RELEASE

The Custodian will provide the Researcher with the records that contain personal health information for the Research Project titled (*insert title)* under the following terms and conditions where the Researcher agrees:

a. to comply with any terms and conditions imposed by a Research Ethics Board;
b. to comply with any terms and conditions imposed by the Custodian;

c. to use the information only for the purposes outlined in the research plan as approved by a Research Ethics Board;

d. not to publish the information in a form where it is reasonably foreseeable in the circumstances that it could be utilized, either alone or with other information, to identify an individual;

e. to allow the Custodian to access or inspect the researcher's premises to confirm that the researcher is complying with the terms and conditions of *PHIA* and of this agreement;

f. to notify the Custodian immediately and in writing if the personal health information is stolen, lost of subject to unauthorized access, use, disclosure, copying or modification;

g. to notify the Custodian immediately and in writing of any known or suspected breach of the agreement between the Custodian and the Researcher; and

h. not to attempt to identify or contact the individuals unless the Custodian or Researcher has obtained prior consent by the individuals.

VI. AMENDMENTS

This Agreement may be amended only by written agreement of the parties.

VII. SIGNATURES

The parties have caused this Agreement to be executed as of the dates indicated below:

_____ _____

(Date) (Signature/Researcher)

_____ _____

(Date) (Signature/Custodian)

Request for Access to Personal Health Information Held by the

_____ (*insert name of custodian)*_____

Definitions from *the Personal Health Information Act (PHIA) and* regulations:

"**custodian"** means an individual or organization described below 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:

(i) a regulated health professional or a person who operates a group practice of regulated health professionals,

(ii) the Minister,

(iii) the Minister of Health Promotion and Protection,

(iv) a district health authority under the Health Authorities Act,

(v) the Izaak Walton Killam Health Centre,

(vi) the Review Board under the Involuntary Psychiatric Treatment Act,

(vii) a pharmacy licensed under the Pharmacy Act,

(viii) continuing-care facility licensed by the Minister under the Homes for Special Care Act or a continuing-care facility approved by the Minister

(ix) Canadian Blood Services,

(x) any other individual or organization or class of individual or class of organization as prescribed by regulation as a custodian

a. Nova Scotia Hearing and Speech Centres

b. a home care agency that is approved by the Department of Health and Wellness and has a service agreement with a district health authority under the *Health Authorities Act* or with the Izaak Walton Killam Health Centre;

c. a home oxygen agency that is approved by and has a service agreement with the Department of Health and Wellness.

"Data linkage" means the bringing together of 2 or more records of personal health information to form a composite record

*"***Data matching**" means the creation of individual identifying health information by combining individual identifying or non-identifying health information or other information from two or more databases without the consent of the individuals who are the subjects of the information

"**Impracticable**" means a degree of difficulty higher than inconvenience or impracticality but lower than impossibility

"**Research**" means a systematic investigation design to develop or establish principles, facts or generalizable knowledge, or any combination of them, and includes the development, testing and evaluation of research

"**Research Ethics Board**" means a research ethics board established and operating in conformity with the Tri-Council Policy Statement

"Tri- Council Policy Statement" means the Tri-Council Policy Statement "Ethical Conduct for Research Involving Humans" adopted in August 1998 by the Medical Research Council or Canada, the Natural Sciences and Engineering Research Council of Canada and the Social Sciences and Humanities Research Council of Canada and includes any amendments or successor statements.

Documents	Version Number	Date (yyyy,mm,dd)
Completed Request Form		
Research Ethics Application & Supporting Documents		
Research Ethics Board Approval		
Research Proposal		
Letters of Support		
Researcher's Current CV(abbreviated)		
Confidentiality Agreement (template attached)		

1. APPLICANT INFORMATION:

Researcher:

Organization:

Address:

Email: Phone: Fax:

Academic Advisor (if Researcher is a student)

Organization:

Address:

Email: Phone: Fax:

2. CO-INVESTIGATORS

List all co-investigators, their affiliation and *specific* role (e.g., data analyst, statistical or clinical consultant, data collection**) in the proposed research project.** If the Researcher is a student, please list all Advisory Committee Members. A signed confidentiality agreement will be required of each individual before the data are released.

1. Name:
Organization:

Primary role on the project including a brief paragraph describing recent similar projects involving the use of personal health information:

Will he/she have access to person identifying data?

- If yes, please provide rationale

2. Name:
Organization:

Primary role on the project including qualifications:

Will he/she have access to line identifying data?

- If yes, please provide rationale

3. Name:
Organization:

Primary role on the project including qualifications:

Will he/she have access to line identifying data?

- If yes, please provide rationale

3. STUDY FUNDER

Has funding been obtained for this study? Yes □ No □

If yes, or pending please indicate the funding source(s):

4. RESEARCH PROJECT

(a) Research Project Title (please include research proposal):

(b) Study objectives/outcome measurers of the Research (please include specific research questions):

(c) Provide, in plain language, a brief summary of your proposed methodology including the analysis plan (maximum 3 pages):

(d) What is the proposed public or scientific benefit of this research?

(e) Are there any foreseeable harms/risks arising from the use of personal health information?

If yes, how will the risks be mitigated?

5. STUDY PARTICIPANTS

(a) Will the study involve direct access to potential study participants? Yes □ No □

i. If no, please move to section 6.

ii. If yes, will the study involve mailing correspondence to potential participants?

Yes □ No □

If yes, include a copy of the introductory letter that will be sent to the potential participants as well as the Information, questionnaires, and any other materials that potential participants will receive.

(b) Will (insert name of custodian) be asked to facilitate a blind mail-out? Yes □ No □

(c) Will participants be asked to provide informed consent for this study? Yes □ No □

If yes, please include consent form**.**

(d) If consent is not being sought, please indicate why.
PHIA requires consent to be sought unless a Research Ethics Board (REB) has determined consent is not required - please see section 57 of *PHIA* for all requirements.

6. SPECIFIC DATA REQUIRED

(a) Please complete the following table which allows (*insert name of custodian*) to clearly identify the objectives and corresponding variables required:

The Personal Health Information Act (*PHIA*) places the highest importance on the protection of privacy and security of the data held by custodians. *PHIA* requires that only the minimum information necessary to accomplish the purpose of the research project be released to researchers. Example provided below.

Variable Required	Clearly define Objective	Rationale	Years of data required	Database/Source
e.g. Age of each person	**e.g.** Do wait times vary for hip replacement surgery in Nova Scotia by age?	**e.g**. To calculate age adjusted incidence rates. Categorized age variable cannot be used for calculating age adjusted incidence rates	**e.g. 1**999-Present	**e.g.** Cancer Registry held by Cancer Care Nova Scotia

(b) Will data from another source(s) be requested for this research study? Yes □ No □

If yes, please provide a list of data sources and the variables requested

(c) Will data held by (*insert name of custodian)* be linked/matched with the above data?

Yes □ No □

If yes, please describe the nature of the linkage, including the process for linking data from varied sources. Please include a flow diagram if multiple linkages will occur, as well as the specific data fields you are requesting.

(d) Estimated time period for need of data: (specify the time: one year, five years, etc. that this data will be used for, or how often this data has to be forwarded to your organization)

7. CONSENT

Will you be obtaining consent from the individuals whose personal health information you are requesting access? Yes □ No □

If no, please provide an explanation as to why seeking consent is impracticable. Please provide supporting documentation presented to the REB that led them to determine that the consent of the subject individuals is not required.

8. INFORMATION PRACTICES

(a) Indicate the physical location where the data will reside (complete address, including room/office number).

(b) Will the data be accessed remotely? Yes □ No□

If yes, by whom? Where is the remote terminal located? What level of data (aggregate vs. line-level) will be accessed? Describe the specific security measures in place to ensure that data security is not compromised by remote access.

(c) Describe the administrative, physical and technical measures taken to safeguard the information. Please include security measures (e.g. physical, technical and administrative controls and safeguards – passwords, firewall, encryption, audits etc.)

(d) Where and how will participants' personal information be stored after the study ends?

(e) How will the information be securely destroyed?

9. PUBLICATION OF THE STUDY RESULTS

Describe how you intend to share and/or publish the results of your research, providing detail on audiences and the format in which data/results will be presented.

For example, the results might be presented to supervising professors, published in academic journals, distributed within an organization, or forwarded to a sponsoring or funding agency; the data/results might be presented in aggregate or de-identified form.

If the results will be published, a copy of the report must be sent to (*insert name of custodian)*

10. CONFLICT OF INTEREST

Will the researcher's interest in the disclosure of the personal health information or the conduct of the research potentially result in an actual or perceived conflict of interest on the part of the researcher? Yes □ No□

If yes, please explain how the researcher intends to address the potential conflict.

11. OTHER INFORMATION

Please describe any other information relevant to this application.

ATTACHMENTS

The following documents must be provided:

□ Research Proposal

□ Research Ethics review application and any supporting documents (all applicable REBs)

□ Research Ethics Board review approval and any interim approvals

□ pending

- □ Peer review support documents, if applicable.
- □ Confidentiality Agreement(s) (template attached)
- □ Researchers' Current CV
- □ Consent Form

DECLARATION

I declare that:

a. This research complies with the Nova Scotia *Personal Health Information Act*;
b. The information received will only be used for the purposes of the study;
c. The research cannot reasonably be accomplished without the use of personal health information;
d. The information is to be used in the most de-identified form possible for the conduct of the research;
e. The protocol ensures the security of the personal health information and its destruction when finished;
f. The researcher's interest in the disclosure of the personal health information or the conduct of the research will not potentially result in an actual or perceived conflict of interest on the part of the researcher except as noted in section 10 (above); and
g. A copy of all published reports and articles will be provided to the (*insert name of custodian).*

Signature of Principal Investigator Date

Confidentiality Agreement for

(*insert custodian & party)*

As a condition of my project work agreement with the (*insert custodian)*

I agree to:

(a) keep private;
(b) treat as being confidential; and
(c) not make public or divulge to any person

any information or material to which I become privy during the term of this project.

I agree to uphold this obligation during, as well as after the completion of my project and abide by all (*insert custodian)* policies.

Any product resulting from my work at the (*insert custodian)* remains property of (*insert custodian)* and cannot be used unless I request to and receive permission from the Manager of the program.

Failure to uphold this obligation of confidentiality will result in my immediate termination with (*insert custodian)*, as well as appropriate communication to (*insert name of privacy officer)* and to my program Chair regarding the breach of confidentiality.

Signed by:

Name **Signature** **Date**

Witnessed by:

Name **Signature** **Date**

INSERT CUSTODIAN'S
LOGO HERE

April 2014

Consent Matrix

	Collection	Use	Disclosure
Express	• Fund-raising • Market research • Marketing for commercial purposes		• Fund-raising, Market research, Marketing for commercial purposes • By a custodian to a non-custodian (unless required or authorized by law) • By custodian to another custodian, if not for the purpose of providing care (unless required or authorized by law) • To the media • To person organization for research purposes (sec 57).
Knowledgeable Implied	• The purpose for which the information was collected or created and all the functions reasonably necessary for carrying out that purpose • A purpose for which this PHIA, another provincial or federal act permits or requires a person to disclose it to the custodian • Educating agents to provide care		• Within the circle of care • A custodian can disclose personal health information to another custodian(s) involved in the individual's health care if: o The information is reasonably necessary for the provision of health care to the individual; and o The individual has not limited or revoked consent to disclosure (under section 17)
None	• Planning and delivering programs or services that the custodian provides or funds in whole or in part, allocating of resources, evaluation or monitoring any of them • Detecting monitoring or preventing fraud of unauthorized receipt of services or benefits related to any of them • ensuring quality or standard of care within a quality review program within the organizations (e.g. not initiated by an individual employee) • Disposing, or modifying the information to conceal identity • seeking the individual's consent, when the info used by custodian is limited to the individuals name and contact information • For the purpose of proceeding or a contemplated proceeding • Obtaining payment or processing, monitoring, verifying or reimbursing claims for payment for the provision of health services • For research conducted by custodian in accordance with sections 52-60 • Subject to requirements and restrictions, if any, that are prescribed, if permitted or required by law or by a treaty, agreement or arrangement made under this *Act* or another *Act* of the Province or of the Parliament of Canada • for purpose of risk management or patient safety within the custodian's organization A custodian may provide personal health information to an agent to use for any of the above purposes (section 35(2)). Agents include employees, volunteers, or the custodian's lawyer.		• To another custodian if the custodian disclosing the information has a reasonable expectation that the disclosure will prevent or assist an investigation of fraud, limit abuse in the use of health services or prevent the commission of an offence under an enactment of a province or Parliament of Canada. • To person(s) acting on behalf of the individual including a SDM (person who is legally entitled to make a health-care decision on behalf of the individual, a legal guardian, or the administrator of an estate, if the use or disclosure is for the purpose of the estate. • To a regulated health professional body or a prescribed professional body that requires information for the purposes of carrying out its duties in the Province under an Act of the province or in another province of Canada or under an Act of that province regulating the profession. • To any person the custodian have reasonable ground to believe that the disclosure will avert or minimize an imminent and significant danger to the health or safety. • To an official of a correctional facility, as defined in the Correctional Services Act, or to an official of a penitentiary in which a person is being lawfully detained, if the purpose of disclosure is to allow the provision of health care to the individual or to assist the correction facility/penitentiary in making a decision concerning correctional services as defined in the CSA or services provided under the Corrections and Conditional Release Act. • To another custodian for the purpose of ensuring quality or standard of care within a quality review program with the custodian's organization • To the Minister of Health and Wellness for the purposes of planning and management of the Health System. • To the NS Prescription Monitoring board under the Prescriptions Monitoring Act. • To CIHI, or another prescribed entity, another province, territory, or the Government of Canada, to assist in the planning and management of the health system in accordance of the terms of an agreement between CIHI and the Province. • Where the disclosure is required or permitted by law or treaty, agreement or arrangement made pursuant to this Act, or another provincial or Federal Act (e.g. in NS-Adult Protection Act, Health Protection Act, Gunshot Wounds Mandatory Reporting Act, or the Children and Family Services Act.) • To another custodian for the purpose of determining eligibility for insured services. • To a person carrying out an inspection, investigation or similar procedure that is authorized by a warrant or under PHIA, or another Act of the province or Parliament of Canada, for the purpose of facilitating the procedure. • To a proposed litigation guardian or legal representative of the individual for the purpose of having the person appointed as such, and to commence, defend or continue a proceeding on behalf of the individual or to represent the individual in a proceeding. • For the purpose of complying with a summons, order, or similar requirement issued in a proceeding by a person having jurisdiction to compel the production of information; or a procedural rule that relates to the production of information in a proceeding. • The disclosure is reasonably necessary for the administration of payments in connection with the provision of health care to the individual or for contractual or legal requirements in that connection. • For the purpose of a proceeding or a contemplated proceeding in which the custodian or an agent or former agent of the custodian is or is expected to be a party or witness, if the information relates to; or is a matter in issue in the proceeding. • For the purpose of risk management or patient safety within the custodian's organization. • To the Minister of Health and Wellness for the purpose of creating or maintaining an electronic health record. • If the information is related to the presence, location and general condition of an individual on the day that the information is requested: family members of the individual; or another person if the custodian has a reasonable belief that the person has a close personal relationship with the individual. • Personal health information about a deceased individual if the information relates to circumstances surrounding the death of the individual or to health care recently received by the individual and the disclosure is not contrary to a prior express request of the individual, to: a family member of the individual; or another person if the custodian has a reasonable belief that the person has a close personal relationship with the individual • information about an individual who is deceased, or believed to be deceased, for the purpose of identifying the individual; informing any person whom it is reasonable to inform that the individual is deceased or believed to be deceased
Limiting/ Withdrawal of Consent	An individual may request to limit or revoke consent for the collection, use or disclosure of their personal health giving notice to the custodian (section 17(1)), however this is not applied retroactively. For example, if an individual informs a custodian that s/he is withdrawing consent to have information disclosed to one of his/her health providers, the custodian is not required to request that any information previously disclosed to the other provider be returned. The custodian must inform the provider named by the individual that the individual's record is not complete, meaning the custodian considers that the information disclosed to that provider is not what is "reasonably necessary" for the care of the individual. The custodian must also inform the individual of the consequences of limiting or revoking consent (section 17(4)), including the fact that the other provider may decide that s/he is not confident in providing care to the individual without understanding what information has been withheld. A custodian is required to take reasonable steps to comply with an individual's request to limit or revoke consent (section 17(3)). In some circumstances it may not be possible to mask information due to technological capabilities. The revocation of consent does not apply to collection, use and disclosure of personal health information that a custodian is required by law to collect, use or disclose (section 17(6)).		

[i] "Research Ethics Board" means a research ethics board established and operating in conformity with the Tri-Council Policy Statement (*PHIA* section 52(d)).

[ii] "Research" means 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 (*PHIA* section 52(c)).

[iii] "Data matching" means the creation of individual identifying health information by combining individual identifying or non-identifying health information or other information from two or more databases without the consent of the individuals who are the subjects of the information (*PHIA* section 52(a)).