***Personal Health Information Act***

**COMPLIANCE CHECKLIST**

This checklist will help custodians under the Nova Scotia *Personal Health Information Act* (*PHIA*) start their privacy analysis to determine whether they have fulfilled their high-level requirements under the *Act*.

Please note that this checklist does not represent an exhaustive list of custodians’ responsibilities under *PHIA*. For further details, please consult the *Act* and any regulations made under the *Act*, which are available for review at [www.novascotia.ca/DHW/PHIA](http://www.novascotia.ca/DHW/PHIA) . Custodians may also choose to seek professional advice regarding their compliance with the *Act.*

Under *PHIA*, custodians are required to:

* prepare and make readily available a notice describing the purpose of the custodian’s collection, use and disclosure of personal health information [**“notice of purposes”**] (s. 15);
* have a **written retention and destruction schedule** for personal health information (s. 50);
* put in place ***“information practices”*** that:
	+ meet the requirements of the *Act* and the regulations;
	+ are reasonable in the circumstances; and
	+ ensure that personal health information in the custodian's custody or under its control is protected against:
		- theft or loss of the information; and
		- unauthorized access to or use, disclosure, copying or modification of the information(s. 62(1)).

*“Information practices”* are defined in the *Act* (s. 3(n)) as *“the policies of the custodian for actions in relation to personal health information, including**:*

1. *when, how, and the purposes for which the custodian routinely collects, uses, discloses, retains, de-identifies, destroys or disposes of personal health information; and*
2. *the administrative, technical, and physical safeguards and practices that the custodian maintains with respect to the information.”*
* implement, maintain, and comply with a **complaints policy** for an individual to make a complaint under this *Act* (s. 62(2)):

A complaints policy must include the following:

* + a requirement that the complaint be submitted in writing;
	+ a statement of the time period following receipt of the written complaint when the custodian must process, investigate and made a decision on the complaint and reply to the complainant; and
	+ the time period referenced above must be no longer than 60 days, unless:
		- the custodian extends the period by no more than 30 days; or
		- a longer extension if approved by the Review Officer.

[Regulation clause 8]

* have the ability to create and maintain a **record of user activity** for any electronic information system it uses to maintain personal health information (s. 63);

A record of user activity must include the following:

* + the name of the individual
	+ a unique identification number, including their health card number or a number assigned by the custodian;
	+ the name of the person who accessed the personal health information;
	+ any additional identification of the personal who accessed the information;
	+ a description of the personal health information accessed or, if this 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 this cannot be determined, a range of dates when the personal health information could have been accessed by the person.

The information used to update a record of user activity must be maintained for one year after each date of access.

[Regulation clause 11]

* designate a ***PHIA*** **contact person** to perform the functions set out in the *Act* (s. 67). [Note: If the custodian is a “natural person” (i.e. an individual health care practitioner), the practitioner may act as the contact person];
* implement **additional safeguards** for personal health information held in an electronic information system, including:
	+ protection of network infrastructure;
	+ protection of hardware and its supporting operating systems to ensure that the system functions consistently and only those authorized have access to the system; and
	+ protectionof the system’s software, including the way it authenticates users’ identity.

In addition, custodians must:

* + create and maintain written policies to support and enforce the safeguard listed above; and
	+ create and maintain a list of every security breach likely to pose a risk to an individual’s personal health information, including details of all corrective action taken to diminish future breaches.

[Regulation clause 10]

* prepare and make available a written statement about the custodian’s information practices, how to reach the contact person, how to request access and correction of the individual’s record, and how to make a complaint [**“written privacy statement”**] (s. 68).

**Templates for the following are available in the Toolkit for Custodians:**

* Notice of Purposes
* Retention and Destruction Schedule
* Complaints Policy
* Written Privacy Statement

For more information about your responsibilities under the *Personal Health Information Act* please consult the *Personal Health Information Act* Toolkit for Custodians available at [www.novascotia.ca/DHW/PHIA](http://www.novascotia.ca/DHW/PHIA) .

You may also contact the Department of Health and Wellness Privacy Office at phia@gov.ns.ca, by calling 902-424-5419 or Toll Free 1-855-640-4765.