PHIA Compliance Checklist for Custodians

The *Personal Health Information Act* (*PHIA*) establishes legal obligations for custodians (including health care professionals and providers) regarding their collection, use, disclosure, and protection of personal health information (PHI).

Protection of PHI

PHIA requires that custodians take steps that are reasonable in the circumstances to protect PHI in their custody or control. What is reasonable will depend on factors such as the sensitivity of the information in your custody or control, the degree of difficulty or cost associated with a particular security measure, etc. Some measures are basic and should be implemented as a matter of course.

Administrative safeguards consist of approved written policies, procedures, standards and guidelines that protect patient, employee, and business information.

Technological safeguards control access to and use of technology such as firewalls, password use, encryption of mobile devices (i.e. laptops and iPads), account restrictions and monitoring.

Physical safeguards consist of physical measures such as locked filing cabinets, keeping computer terminals and white boards away from public areas, and restricting access to unauthorized personnel.

All safeguards should be periodically assessed to ensure they are still effective and still meet the reasonableness standard set out in *PHIA*. This is particularly true for technical safeguards, given the rapid pace at which technology advances.

Access to or Correction of PHI

Patients have a right of access to their own PHI under *PHIA*. Requests for access can be made directly to you or to one of your staff and may be verbal or in writing. A request must contain sufficient information to allow you to locate the records. If it does not, you have a duty to assist the patient in clarifying their request. The response deadline for access requests is 60 days, unless an extension is allowed under the *Act*.

If you refuse access (section 58 sets out specific and limited options for refusing access), the patient may file a complaint with our Office or proceed to Court.

If access is granted, a reasonable fee may be charged for providing access.

Patients also have a right to have their PHI corrected. They may make a request for correction to you directly or to one of your staff, in writing or verbally, and you must respond within 30 days, unless an extension is allowed under the *Act*.

Office of the Information and Privacy Commissioner
P.O. Box 13004, Station "A", St. John's, NL A1B 3V8
Telephone: (709) 729-6309 or 1-877-729-6309 Fax: (709) 729-6500
E-mail: commissioner@oipc.nl.ca www.oipc.nl.ca

If you refuse to correct the information, you must make a note that a request for correction was made and advise the patient why you refused.

Section 62 sets out the reasons for refusing to correct that are permitted under *PHIA*. A refusal to correct information in a record may be appealed to this Office or to Court.

Privacy Breach

A privacy breach is any collection, use or disclosure of personal health information that is not authorized under *PHIA* (including theft or loss). For example, PHI may be lost (a patient's file is misplaced), stolen (a laptop computer is taken from your office) or inadvertently disclosed to an unauthorized person (a letter addressed to patient A is actually mailed to patient B). However, a Custodian may also become aware of breaches that are intentional; for example, an unauthorized access of patient files by staff.

If the privacy breach is a material breach it must be reported to the OIPC. Section 5 of the *Personal Health Information Regulations* of *PHIA* outlines the factors that are relevant in determining what constitutes a material breach, including the sensitivity of the information involved, the number of people whose PHI was involved, the potential for the information to be misused and whether the cause of the breach indicates a systemic problem.

Education and Training

Finally, as a Custodian, you are also responsible for ensuring that your employees, agents, contractors and volunteers are aware of their obligations under *PHIA* and of your policies and procedures that support the legislation.

What follows is a quick checklist to help get you thinking about your obligations under *PHIA* and how well you are meeting these obligations.

If you have any questions or would like more information, we would be happy to meet with you and discuss these issues further. We can be reached at 729-6309 or commissioner@oipc.nl.ca.

PHIA Compliance Checklist for Custodians

Question	Y, N, or N/A	Follow Up Questions and Considerations
1. Do you have policies in place regarding PHI?		For collection? Protection? Storage? Transfer? Copying? Modification? Use? Disposition?
2. Do you have confidentiality agreements for employees, contractors and volunteers?		Sign Oath/Affirmation? Updated? Confidentiality clause in contracts with third parties?
3. Are your employees aware of their obligations? Has there been privacy training?		Do you track involvement in training? Is it updated? Are they aware of the consequences of breaching *PHIA* or your policies?
4. Do you have reasonable physical security measures in place?		Locked cabinets? Restricted access? Privacy screens on monitors? White boards and appointment books positioned so they cannot be seen easily by the public? Cautioned about overhearing?
5. Do you have reasonable technical security measures in place?		Firewalls and virus scanners? Strong passwords? Document tracking? Tracking and audit procedures for electronic access? Encryption? Limited access to as needed? Logging off/timeout?
6. Do you have reasonable administrative security measures in place?		Limits on faxing or emailing PHI? Preprogrammed fax machine? Kept up to date? Do you use an EMR? Did you do and update a Privacy Impact Assessment? Voicemail rules? Social media awareness?
7. Do you have a *PHIA* public written statement posted or provided?		Does it include a description of your policies? Contact person information? Information on how to access their PHI? How to complain?
8. How well do you inform your patients of their rights under *PHIA*?		Do you inform them of the purpose of collection? Get their consent before disclosing? Advise them of how to access their own information, including fees? Advise them of their right to correction?
9. How aware are you of what to do in case of a privacy breach?		Do you know what constitutes a breach? A material breach? Do you know your obligations? Have you taken any steps to avoid a breach?
10. Have you designated a contact person?		Is the contact information for that individual listed on your written public statement? Is this person aware of their responsibilities?
11. Do you have an Information Manager? If so, do you have an Information Management Agreement with your Information Manager?		Has your Information Manager signed an Oath/Affirmation? Updated? Is there a Confidentiality clause in the agreement?
12. Do you keep a record or log of all disclosures of PHI?		Where is the log maintained? Who is responsible for maintaining the log? What information is captured (i.e. to/from; date; reason for disclosure; number of pages, etc.)