Office of the Information and Privacy Commissioner for Nova Scotia

PHIA – Rules Summary and Checklist for Custodians

The *Personal Health Information Act* (*PHIA*) sets out the obligations of custodians and their agents regarding the collection, use, disclosure, and protection of personal health information (PHI). This document produced by the Office of the Information and Privacy Commissioner for Nova Scotia (OIPC)[1] is intended to provide custodians with a brief summary of the key rules in *PHIA* and a quick way to assess compliance with the privacy management framework expected by *PHIA*. It should not be taken as a comprehensive or definitive guide on how to fulfill your responsibilities as a custodian.

Staff at the OIPC are available to consult on specific questions related to *PHIA*. Please contact us by phone at 902-424-4684, by email at oipcns@novascotia.ca, or visit our website at www.foipop.ns.ca.

Definitions	
Custodian	• A custodian is an individual or organization that has custody or control of an individual's PHI for the purpose of providing the individual with health care. • Custodians include regulated health professionals, health authorities, pharmacies, continuing care facilities and other organizations. • A regulated health professional is not a custodian when he or she is working as an agent of a custodian. For example, where a physician works in a health authority hospital, the health authority is the custodian, and the physician is an agent. • The obligations under *PHIA* fall on the custodian.
Agent	• Agents are people who are authorized by the custodian to handle PHI for the custodian. Agents would include the custodian's staff and contractors. • Custodians must limit agents' access to individuals' PHI to those agents who need to know the information to do their jobs. • An agent is required to follow the rules set by the custodian, and to notify the custodian at the first reasonable opportunity if the agent learns of a privacy breach.
Personal health information (PHI)	• Personal health information (PHI) means identifying information about an individual if the information relates to the health care sought by or provided to the individual. • Identifying information means any information that either directly identifies the individual or could reasonably be combined with other information to identify an individual. • PHI includes: ▪ information about the individual's health, including his or her family history; ▪ the assessment of a health care issue, and the provision of treatment by a regulated health professional; ▪ the identification of a regulated health professional as an individual's health care provider; and ▪ the individual's test results and registration information.

[1] The Information and Privacy Commissioner for Nova Scotia is also known as the Review Officer and is appointed as the independent oversight authority under the *Freedom of Information and Protection of Privacy Act*, the *Municipal Government Act*, the *Personal Health Information Act* and the *Privacy Review Officer Act*.

Rules	
Consent	• The basic rule is that consent is required for collection, use and disclosure of PHI. The collection, use or disclosure must also be reasonably necessary for the lawful purposes of the custodian. In short, the custodian will need to be able to connect the processing of PHI to its health care purposes, or business activities to support those purposes. • The custodian can rely on "knowledgeable implied consent" to collect, use or disclose the individual's PHI. • Knowledgeable implied consent is achieved if the custodian clearly explains the purpose of the collection, use or disclosure of PHI. The explanation can either be verbal or through a readily-available written notice. (Note that the written notice will be insufficient in cases where the custodian should have known about the individual's limited literacy in English).
Collection, use and disclosure	• The basic rules for all collection, use and disclosure of PHI are that the custodian only uses PHI when it is necessary, and only processes the minimum amount of PHI necessary for the task. • The custodian can disclose a patient's PHI to another custodian involved in the individual's "circle of care." For instance, when referring a patient to a specialist. • In certain specific circumstances, collection, use and disclosure can happen without an individual's consent (see *PHIA* sections 31, 35, and 38, respectively).
Rules for protection of personal health information	
Protection of PHI	• A custodian is required to take reasonable steps to protect the confidentiality of personal health information in its custody or control as well as the privacy of the individual to whom the information relates. • 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 without second thought – for instance, keeping cabinets and doors locked. All safeguards should be periodically reassessed 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.
Safeguards	• *Administrative safeguards* (also called procedural controls) consist of approved written policies, procedures, standards and guidelines that protect patient, employee, and business information. • *Technology safeguards* consist of controls on access to and use of technology such as password use, regular software patching, firewalls, antivirus software, ensuring encryption of mobile devices (i.e. laptops and iPads), and logging off computers. • *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. • The OIPC has produced a "Reasonable Security Checklist for Personal Information" (direct link) that provides a more detailed summary of reasonable security requirements.

Patient rights	
Access to PHI	• Patients have a right of access to their own PHI under *PHIA*. Requests for access are made directly to the custodian and may be verbal or in writing. • Access requests must contain sufficient information to allow the custodian to locate the records. If they do not, the custodian has a duty to assist the patient in clarifying his or her request. • The response deadline for access requests is 30 days, unless an extension is allowed under *PHIA*. • If the custodian refuses access (a list of reasons to do so are set out at section 72) the individual may file a complaint with the OIPC. • If access is granted, the Regulations specify the fees that may be charged for providing access. The OIPC has produced a "PHIA Fee Fact Sheet" (direct link) that summarizes the regulations.
Correction of PHI	• Patients also have a right to have their PHI corrected. They make a request for correction to the custodian directly, in writing or verbally. • The custodian must respond within 30 days, unless an extension is allowed under *PHIA*. • If the custodian refuses to correct the information, it must make a note that a request for correction was filed and advise the patient the reasons for refusal. • Section 87 sets out the reasons for refusing to correct that are permitted under the *Act*. • If the custodian refuses to correct a record, the individual may file a complaint with the OIPC.
Privacy complaint	• A custodian is required to have a privacy complaints policy and a designated contact person who can receive and process privacy complaints. • Privacy complaints are filed in writing directly to the custodian. • The custodian determines the response deadline for privacy complaints, but that deadline must be no more than 60 days after receiving the complaint, unless an extension is allowed under *PHIA*. • If the individual is unsatisfied by the custodian's response, he or she can complain to the OIPC.
Privacy breach management	
Privacy breach	• A privacy breach is any handling of PHI that is not authorized under *PHIA*. 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). • A custodian may also become aware of breaches that are intentional; for example, an unauthorized access of patient files by staff.
Investigating a breach	• The OIPC has produced a document, "Key Steps to Responding to Privacy Breaches" (direct link) to help custodians investigate breaches. OIPC staff are also available to assist a custodian work through this analysis. We can be reached by phone at 902-424-4684, by email at oipcns@novascotia.ca or through our website at www.foipop.ns.ca.

Breach notification	• Sections 69 and 70 of *PHIA* outline the requirements for reporting a privacy breach. The custodian is obligated to report a privacy breach either to the individual whose PHI has been breached or to the OIPC. • The individual must be notified if there is potential for harm or embarrassment resulting from the breach; if not, the custodian may choose to notify the OIPC.

What follows is a quick checklist to help get you thinking about your obligations under *PHIA* and how well you are meeting these obligations. It should not be taken as a comprehensive or definitive guide on how to fulfill your responsibilities as a custodian. If you have any questions or would like more information, we would be happy to discuss these issues further. We can be reached at 902-424-4684 or oipcns@novascotia.ca.

Question	Y, N, or N/A	Follow Up Questions
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? Information Manager agreement?
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/as needed access controls? Logging off/timeout?
Question	**Y, N, or N/A**	**Follow Up Questions**
6. Do you have reasonable administrative security measures in place?		Limits on faxing or emailing PHI? Pre-programmed fax machine? Kept up to date? Do you use an EMR? Did you do and update a privacy impact assessment (PIA)? 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? Do you know your obligations? Have you taken any steps to avoid a breach?

To conduct a complete assessment of your privacy management program, the OIPC has produced the Privacy Management Program Toolkit for Health Custodians (direct link). OIPC staff are available to consult on a custodian's Privacy Management Program and can be reached by phone at 902-424-4684, by email at oipcns@novascotia.ca, or through our website at www.foipop.ns.ca.

Notice

Please note that as an independent agency mandated to oversee compliance with *PHIA*, we cannot approve in advance any proposal from a health custodian. We must maintain our ability to investigate any complaints and to provide recommendations in response to these complaints. Therefore, when we are consulted by a health custodian, we provide comment and may even make suggestions for the consideration of the health custodian. These suggestions should not be viewed as an approval or endorsement by this office. Our comments or suggestions do not fetter or bind this office with respect to anything on which we have commented. It remains the responsibility of health custodians to ensure that they comply with their responsibilities under *PHIA.*