Guidelines for Custodians
– to assess compliance with the *Personal Health Information Privacy and Access Act (PHIPAA)*

This document is designed to help custodians evaluate readiness for compliance with PHIPAA and to help identify where policies or practices may need to be developed and/or changed to ensure compliance. It is intended to complement the document entitled: *Preparing for the Personal Health Information Privacy and Access Act (PHIPAA): a checklist for custodians.*

NOTE: This document is a guide only; it is not intended to provide a complete statement of your organization's legal obligations and as such it should not be construed as legal advice. Reference should always be made to the official text of PHIPAA and its regulations for a complete statement of the law and for further information about the points presented here. The relevant sections of the Act are referenced in parentheses throughout the document to assist you.

1. Are you a "custodian" as defined by PHIPAA? *(Section 1)*

PHIPAA applies to personal health information that is collected, used or disclosed by a custodian or that is in the custody or control of the custodian. "Custodian" means an individual or organization that collects, maintains or uses personal health information for the purpose of providing or assisting in the provision of health care or treatment or the planning and management of the health-care system or delivering a government program or service and includes:

(a) public bodies,
(b) health-care providers,
(c) the Minister,
(d) the following organizations or agencies:
- *(i) Ambulance New Brunswick Inc.,*
- *(ii) the New Brunswick Health Council,*
- *(iii) FacilicorpNB Ltd.,*
- *(iv) regional health authorities,*
- *(v) WorkSafeNB*
- *(vi) Canadian Blood Services,*

(e) information managers,
(f) researchers conducting a research project approved in accordance with this Act,
(g) health-care facilities,
(h) a laboratory or a specimen collection centre,
(i) nursing homes and operators as those terms are defined in the Nursing Homes Act, and
(j) a person designated in the regulations as a custodian.

Yes	No	
☐	☐	Are you (or is your organization) a custodian as defined above?

2. Do you collect, use, disclose or maintain personal health information that may be subject to PHIPAA? *(Sections 1 and 3)*

PHIPAA applies to personal health information that is collected, used, maintained or disclosed by a custodian or that is in the custody or control of the custodian. Personal health information is defined in part as identifying information about an individual pertaining to that person's mental or physical health, family history or health care history. This includes:

- genetic information;
- registration information, including the Medicare number of the individual;
- information about payments or eligibility for health care or health-care coverage;
- information pertaining to a donation by the individual of any body part or bodily substance;
- information derived from the testing of a body part or bodily substance of the individual; and
- information that identifies the individual's health-care provider or substitute decision maker.

Certain records and information containing personal health information may not be subject to PHIPAA. Please refer to Question 3 and also consult the Act for more information.

Yes	No	
☐	☐	Do you have records containing personal health information?

3. Do the exceptions defined in PHIPAA, which exclude personal health information from the application of PHIPAA, apply to the personal health information in your custody or control? *(Sections 3 and 4)*

The Act provides for certain instances whereby personal health information will be excluded from the application of PHIPAA and the Act will not apply. For example, the Act does not apply to:

- an individual or organization that collects, maintains or uses personal health information for purposes other than health care or treatment and the planning and management of the health-care system, or for delivering a government program and service including: employers (public and private), insurance companies, regulatory bodies of health-care providers, licensed or registered health-care providers who do not provide health care, and certain other individuals or organizations prescribed by regulation;
- personal health information in a record created 100 or more years ago or where 50 or more years have passed since the death of the individual;
- information in a court record, such as a record of support services provided to a judge or court official;
- a record created or information held by a person under the provisions of certain other Acts of the Legislative Assembly, including the *Family Services Act,* the *Mental Health Act,* and any other Act of the Legislative Assembly prescribed by regulation.

Consult the Act and regulations for more information on instances where PHIPAA may not apply.

Yes	No	
☐	☐	Check "yes" if there are exceptions that may exclude the personal health information in your custody or control from the application of PHIPPA.

Your answers to Questions 1, 2, and 3 may be used to assess whether PHIPAA will apply to all or some of the personal health information in your custody or control. For a more comprehensive assessment of the application of PHIPAA in your specific circumstances, consult the Act and regulations.

4. Rights of the individual

4.1. Obtaining consent *(Sections 17, 18, 19)*

4.1.1 General considerations regarding consent

Yes	No	
☐	☐	Have you obtained consent from the individual for the collection, use or disclosure of personal information unless otherwise required or permitted by the Act or by law?
☐	☐	Is consent knowledgeable? *(for consent to be knowledgeable, individuals must be informed (by way of a readily available notice or similar means) in laymen's terms about the purpose of the collection, use or disclosure of their information both within and outside of the circle of care and informed of their right to withhold or withdraw their consent)*
☐	☐	Is consent specifically related to the personal health information collected and the purpose(s) for which it will be used?
☐	☐	Is consent voluntary *(consent may not be coerced)*?

4.1.2 Express consent

Yes	No	
☐	☐	Where applicable, have you obtained express consent for the collection, use or disclosure of personal health information? *(Where consent is required by the Act, it must be express unless the Act specifically permits an implied consent – see 4.1.3 below).*

Express consent will generally be required when information is being disclosed to any of the following (unless otherwise provided in the Act):

√ the media;

√ a person for the purpose of fund-raising;

√ a visitor to a health-care facility;

√ a person for a non-health care related purpose (for example, information disclosed to an insurance company);

√ a person outside of New Brunswick (some exceptions apply – refer to Section 47); and

√ a person for the purpose of research (some exceptions apply – refer to Section 43).

Yes	No	
☐	☐	Will you ensure the express consent is obtained in writing from the individual or his or her substitute decision-maker?
☐	☐	Have the general considerations for consent outlined in 4.1.1 been met?

4.1.3 Implied consent

Yes	No	
☐	☐	Is there implied knowledgeable consent of the individual to share his/her personal health information within the circle of care for providing health care to that individual? *(For implied knowledgeable consent to exist, it must be reasonable to assume that the individual understands the purpose for the collection, use or disclosure of his or her personal health information within the circle of care and the implications of providing or withdrawing consent).*
☐	☐	Have the general considerations for consent outlined in 4.1.1 been met?

4.1.4 Consent not required

Yes	No	
☐	☐	If you will collect, use or disclose personal health information without consent, has the authority under the Act to do so been documented and confirmed?
☐	☐	Do you have a process in place to ensure there is a record of all personal health information disclosed without consent under the Act as required by Section 46?

4.2. Consent Directives *(Section 22)*

Yes	No	
☐	☐	Where consent has been obtained, are there procedures in place to address an individual's request to withdraw consent to the collection, use or disclosure of his or her personal health information?
☐	☐	Are procedures in place to control and monitor situations where a custodian may be required to override an individual's consent directive in accordance with the Act (for example, for health and safety reasons)? *(procedures should include, but not be limited to: logging, monitoring and auditing consent directive overrides to ensure that they are documented and authorized by the Act).*
☐	☐	If information networks are used, is a process in place to inform individuals about how they can exercise their right to prevent access to or disclosure of their personal health information contained in an information network? *(note, however, that an individual may not withhold his or her consent for the collection of personal health information by a custodian for creating and maintaining an information network).*

4.3 Right to be informed *(Section 31)*

Yes	No	
☐	☐	Have you taken reasonable steps to directly inform individuals whose personal health information is being collected directly of the purpose (including anticipated uses and disclosures) for which the information is being collected before or as soon as practical after it is collected? *("Reasonable steps" may include, for example, creating a poster or a privacy notice and making it available on the custodian's website or as a handout; notifying individuals either verbally or in writing about how they may obtain a copy of the organization's privacy notice; and describing the purpose of collection on forms used to collect personal health information.).*

4.4. Collecting the Medicare number *(Section 48)*

Yes	No	
☐	☐	Are individuals only required to produce their Medicare number for reasons connected to health services?
☐	☐	If you require the Medicare number for non-health purposes, is the collection authorized by an Act or regulation? *(If not, collection can be voluntary, but cannot be made as a condition of receiving a service. Individuals must have the option of using other identification).*

4.5. Individual's right to complain to the Access to Information and Privacy Commissioner regarding an action/decision of a custodian *(Part 6)*

Yes	No	
☐	☐	Are individuals informed of their right to contact the Access to Information and Privacy Commissioner to request a review of an action taken or a decision made in the event that you cannot resolve a concern regarding their personal health information?

4.6. Individual's ability to designate a substitute decision-maker *(Sections 25,26)*

Yes	No	
☐	☐	Do you have procedures to process an individual's written request to designate another individual to act on his or her behalf regarding his or her rights pertaining to his or her personal health information?
☐	☐	If an individual is not able to act on his or her behalf; do you ensure that the designated person meets one of the circumstances identified in Section 25 of the Act?

4.7. Requests for access to personal health information *(Part 2, Division A)*

Yes	No	
☐	☐	Have you established procedures to receive requests for, and provide access to records containing personal health information?
☐	☐	Will you charge a fee for providing access? If so, is it consistent with the regulations under PHIPAA?
☐	☐	When responding to requests for disclosure of personal health information do you have procedures in place to uniquely identify the individual to whom the information relates before granting access to the information?

4.8. Requests to correct personal health information

Yes	No	
☐	☐	Have you established procedures to correct records of personal health information when required by the individual about whom the information pertains; or to place a statement of disagreement on the records of the individual's personal health information?

5. Protection of personal health information

5.1. Duty to protect (Section 50)

Yes	No	
☐	☐	Have you developed a security policy and supporting procedures that outline how your organization will ensure that reasonable safeguards are in place to protect the *confidentiality, security, accuracy and integrity* of the personal health information in your custody or control?
☐	☐	Has a review been conducted to ensure that information practices and policies conform with industry standard (national or jurisdictional) information technology security standards and processes appropriate for the level of sensitivity of the personal health information to be protected?
☐	☐	Have you implemented reasonable physical safeguards such as locked cabinets and use of access cards to control entry to storage areas that contain personal health information?
☐	☐	Have you implemented reasonable administrative safeguards such as background checks, mandatory employee training and appropriate privacy and security policies to protect personal health information against risks such as unauthorized access, use, disclosure or modification?
☐	☐	Have you implemented reasonable technical safeguards such as appropriate encryption of personal health information, strong passwords, anti-virus protection and firewalls to protect personal health information against unauthorized access, use, disclosure or modification?
☐	☐	Are the policies and procedures described above designed to protect information in all forms including, but not limited to paper records; computer records including databases, e-mail, electronic forms; and microfilm/fiche?

5.2. Retention, storage and secure destruction (Section 55)

Yes	No	
☐	☐	Do you have written policies for the retention, archival storage, access and secure destruction of personal health information in your custody and/or control?
☐	☐	Do your existing procedures enable compliance with such policies?
☐	☐	Do retention policies comply with any applicable legislative requirements?
☐	☐	Do the above policies apply to records in all formats (for example,. paper, electronic databases, e-mail, microfilm/fiche) regardless of media?
☐	☐	Are there policies or procedures that ensure personal health information is securely destroyed when no longer required? *(Policies should mitigate risks such as records containing personal health information thrown in a garbage can or electronic records not completely removed from a hard drive sold for salvage).*
☐	☐	Do you have a formal /secure system and process to backup electronic data contained on all computer systems that store personal health information?
☐	☐	Are backup tapes securely stored and appropriately destroyed once they have reached the end of their useful life?

Yes	No	
☐	☐	Do you ensure paper records are safely stored where they will not suffer damage from risks such as flooding/water damage?
☐	☐	Do you keep a formal record of the contents of all records containing individuals' personal health information destroyed in accordance with the retention and/or destruction policy?
☐	☐	Is personal health information in the organization's custody or control stored outside Canada only for authorized purposes *(storage outside of Canada is not permitted unless the individual has consented or unless such storage is specifically authorized under the Act)?*

5.3. Information Management Service Provider agreements (Section 52)

Yes	No	
☐	☐	Have you identified all "information managers" (for example, paper shredding services, IT service providers) engaged by your organization in delivering programs and services?
☐	☐	Do you have written agreements with all information managers that contain appropriate privacy and security clauses including: • a description of how the personal health information will be protected against risks such as unauthorized access to or use or disclosure of the information, unsecure destruction or alteration; • the requirement for the information manager to comply with the PHIPAA and regulations; • the requirement that information managers do not store personal health information outside of Canada except in the case of maintenance and technical support provided for personal health information systems or unless otherwise provided for in the Act.

5.4. Duty to collect accurate information (Section 53)

Yes	No	
☐	☐	Do you take reasonable steps to ensure that the personal health information you collect is accurate and complete?

6. Collection, use and disclosure

6.1. Limitations on collection (Section 29)

Yes	No	
☐	☐	Do you take steps to limit the personal health information that is collected, used or disclosed to only what is necessary to satisfy the purpose of the collection, use or disclosure?
☐	☐	Do you use or disclose de-identified personal health information if it will serve the purpose as identifiable information?

6.2. Manner of collection *(Section 28)*

Yes	No	
☐	☐	Do you only collect personal health information directly from the individual about whom that information pertains?
☐	☐	If personal health information is collected indirectly from other sources, has the individual consented to collection by the other means or does the collection fall under one of the exceptions specified in Section 28 of the Act?
☐	☐	When collecting personal health information from other sources, do you take reasonable steps to verify the accuracy of the information?

6.3. Restrictions on use and disclosure *(Sections 32-45)*

Yes	No	
☐	☐	Do you have policy or procedures to limit the use and disclosure of personal health information to the minimum amount of information necessary to accomplish the purpose for which it is to be used or disclosed?
☐	☐	Do you have policy or procedures to restrict access to or disclosure of an individual's personal health information by persons such as employees, volunteers and others who do not need to know the information to perform their jobs?
☐	☐	Do you have consent from individuals for every use of their personal health information?
☐	☐	If you do not always have consent to use an individual's personal health information, does the use meet one of the criteria outlined in Section 34 of the Act ?
☐	☐	Do you take steps to ensure that consent is obtained prior to disclosing personal health information unless the disclosure is specifically authorized by the Act?
☐	☐	If you do not have consent to disclose an individual's personal health information, is the reason for disclosure one of the circumstances identified in Section 37(6) and Sections 38-45 of the Act? (*These sections allow limited disclosure without consent.)*
☐	☐	Do you inform non-custodians that they can only use personal health information for the purpose(s) for which you are disclosing it to them and for no other reason, except where permitted by the Act?
☐	☐	Do you have a policy requiring that personal health information be de-identified in circumstances where consent for use or disclosure has not been obtained and where the use or disclosure of personal health information is not authorized by the Act?
☐	☐	In the case where de-identified information will be used or disclosed, do you have procedures in place to provide reasonable assurance that the information cannot be used either alone or in combination with other information to re-identify an individual or individuals whose personal health information is contained in the data set?

6.4. Use or disclosure for research (Section 43)

Yes	No	
☐	☐	Will personal health information be used or disclosed for research?
☐	☐	If personal health information is to be used or disclosed for research, has the project been approved by an authorized research review body having met all of the requirements of the Act?

7. Other things to consider – general privacy practices

7.1. Responsibility for privacy

Yes	No	
☐	☐	Have you designated one or more individuals who will be responsible for implementing and overseeing compliance with PHIPAA? *(individual(s) should be appropriately trained and be provided with adequate resources to do the job)*

7.2. Privacy policy – development and compliance

Yes	No	
☐	☐	Do you have a written privacy policy intended to ensure compliance with the Act within your organization?
☐	☐	Are staff and contractors familiar with the privacy policy, and are they periodically reminded of their responsibilities for compliance with the policy?
☐	☐	Are staff and contractors required to sign confidentiality agreements that contain a written requirement for them to comply with PHIPAA and the organization's privacy policies?
☐	☐	Are procedures in place to monitor and ensure agents' (for example, employees', contractors', volunteers') compliance with the organization's privacy and security policies?

7.3 Privacy Notice

Yes	No	
☐	☐	Have you developed a publicly displayed privacy notice for your organization that will provide individuals with reasonable notice of your organization's privacy practices?

(A privacy notice may be made available, for example, on the organization's website, incorporated within posters and brochures, or by way of voice recording). A privacy notice is a communication tool that is different than (but must be consistent with) the organization's privacy policy. The privacy policy is an internal document that outlines employees' and agents' responsibilities for privacy under the legislation.

☐	☐	Have you reviewed the organization's forms, applications, etc., that are used to collect personal health information to ensure that individuals are appropriately informed about the purposes for the collection of the information at the time it is provided? This may be done either by incorporating an explanation of the purpose directly within the forms or by a short statement explaining how the individual may obtain a copy of the privacy notice or obtain more information about the purpose of the collection.

7.4. Privacy training and awareness

Yes	No	
☐	☐	Do you have a plan in place to regularly deliver mandatory privacy training to all employees and contractors to reinforce their obligations under PHIPAA and the organization's privacy policies?
☐	☐	Do you have a plan in place to communicate the organization's privacy policies to employees and to assist employees/managers develop procedures that support alignment with the policies?

7.5. Privacy inventory and gap analysis

Yes	No	
☐	☐	Have you completed an inventory of your organization's information holdings and identified the various purposes for which you collect, use and disclose personal health information?
☐	☐	Have you conducted a gap analysis based on the inventory to determine areas of risk and non-compliance?

7.6. Investigation of privacy incidents and breaches

Yes	No	
☐	☐	Do you have a process for receiving and investigating privacy complaints in a timely manner?
☐	☐	Have you developed a privacy incident response policy and procedures to manage and contain a privacy breach should it occur?
☐	☐	Have you developed a process for reporting a privacy breach to the Access to Information and Privacy Commissioner and for notifying the affected individual(s)?