Preparing for the *Personal Health Information Privacy and Access Act* (PHIPAA):

a checklist for custodians

This checklist is designed to help custodians identify some key actions they can take to assess their readiness for complying with the *Personal Health Information Privacy and Access Act* (PHIPAA). It is a guide only; it should not be construed as legal advice. Custodians are encouraged to consult PHIPAA and its regulations for a complete statement of the law. They may also wish to seek professional advice in further assessing their compliance with PHIPAA.

√ Designate someone to oversee PHIPAA compliance

Designate an individual accountable for ensuring overall compliance with PHIPAA, including:

- √ developing and implementing appropriate privacy policies and procedures;
- √ monitoring compliance with the organization's privacy policy;
- √ educating employees and other agents about privacy and security;
- √ ensuring that appropriate written agreements with third party agents and information managers are in place; and
- √ responding to inquiries/concerns about how personal health information (PHI) is managed.

√ Review and assess information-handling practices and address risks

Review

- √ complete an inventory of all PHI that is collected, used, disclosed, maintained, and destroyed;
- √ identify the information needs of the different functions/programs within the organization; and
- √ identify current information practices (including why and how PHI is collected, used, maintained, disclosed, and destroyed).

Assess

- √ consider whether the information-handling practices meet PHIPAA obligations and
- √ identify and assess privacy risks presented by current information practices.

Address

- √ develop a plan to close gaps, starting with the highest-risk areas;
- √ consider what changes should be made to policies and practices and whether new ones are needed; and
- √ consider whether security safeguards (technical, physical and/or administrative controls) are appropriate in relation to the level of risks of breach to privacy.

√ Develop or update the organization's information policies including:

- √ privacy policy (address collection, use, disclosure, access and correction, complaints handling, consent management, safeguards, retention, disposal, and accuracy);
- √ security policy (ensure IT security standards are appropriate for the sensitivity of the information being protected and conform with best practice security standards);
- √ retention policy;
- √ user access policy (how user access to PHI will be granted, monitored and removed);
- √ policy/procedure for secure destruction of PHI;
- √ breach notification / incident response policy and procedure; and
- √ policy on access to and correction of PHI.

√ Promote and monitor compliance of staff and third parties with policies

- √ educate staff and third parties about their obligations for complying with information policies and with PHIPAA and how this relates to their day-to-day work;
- √ require all new employees and third parties to undergo mandatory privacy and security training before being given access to PHI.
- √ require employees and third parties to sign a confidentiality agreement requiring them to comply with PHIPAA and the organization's privacy and security policies;
- √ require employees and third parties to review and sign off each year on their compliance with the organization's privacy and security policies; and
- √ implement processes whereby system and program compliance with PHIPAA will be regularly monitored.

√ Develop or revise the privacy notice, forms and communications materials

- √ develop a privacy notice to inform patients/clients about your privacy practices;
- √ make the notice available /visible to individuals when their information is collected. This could be on the organization's website, within posters, brochures, handouts, etc.; and
- √ review forms that are used to collect PHI to ensure individuals are appropriately informed about the organization's information practices or directed to the privacy notice.

√ Review and revise contracts and agreements to comply with PHIPAA

- √ identify "information managers" (for example, paper-shredding services, IT service providers, government service organizations) that process PHI on your behalf; and
- √ update or create written agreements or contracts with information managers describing:
  - √ the purpose for which they are allowed to use PHI and prohibiting other uses or disclosures;
  - √ how the PHI is to be protected while in their custody or control;
  - √ if applicable, how the PHI is to be destroyed in a secure manner without compromising the confidentiality of the PHI;
  - √ the requirement for the information manager to comply with the Act and regulations; and
  - √ restrictions on storing PHI outside Canada (subject to certain exceptions).

√ Create an effective process for handling privacy incidents and breaches

- √ develop procedures for receiving and responding to complaints about privacy practices.
- √ develop procedures for escalating and investigating privacy concerns and incidents within your organization and for responding to, and appropriately reporting privacy breaches.
- √ Develop procedures for notifying individuals whose privacy has been breached, including time, and method.
- √ Develop methods to track privacy breaches, large or small, in order to continually improve safeguards in place and in order to prevent future breaches.

√ Be ready to respond to individuals' access and correction requests

- √ define and publish in the organization's privacy notice and its policy how individuals can obtain access to and request corrections to their PHI.
- √ create procedures for granting access to/correction of records including to whom requests are directed, when they are transferred, how fees will apply, how identity will be verified, and how statements of disagreement will be obtained and recorded.

√ Develop and document a consent management process

- √ determine the applicable consent model(s). Document when implied knowledgeable consent will apply, when you will need to obtain express consent, and circumstances, if any, which permit you to collect, use or disclose information without consent;
- √ if information is being disclosed without consent, ensure that you appropriately document the nature of information disclosed as required by the Act; and
- √ design procedures to enable individuals to communicate consent directives. Outline how such directives will be managed, including when it may be necessary to override a consent directive and how these instances will be documented and monitored.

√ Review PHIPAA to identify other provisions that may apply such as:

- √ restrictions on collection and use of the Medicare number;
- √ the requirement to complete a Privacy Impact Assessment (PIA) if you are a public body;
- √ rules applicable to custodians who create or operate within an information network;
- √ ceasing operation as a custodian;
- √ substitute decision-makers and the exercise of rights by a personal representative; and
- √ use and disclosure of PHI for research.