941812

GBJA
GBJA-E-1
GBJA-E-2
GBJA-E-3
GBJA-E-4

Access and Privacy Management Plan

Personal Information

What is considered personal information?

Personal information is any recorded information about an identifiable individual. Examples include a person's name, address, telephone number, a number that can identify them (for example, case file number, credit card number or social insurance number), and financial information.

Personal health information is any recorded information about an identifiable individual in the healthcare context. Examples include an individual's name, address, telephone number, or personal health identification number (PHIN).

It is important to note that personal (health) information can include information that can be combined with other information to identify a specific individual. For example, if information such as gender were linked to health information and only one individual in a small office was of that gender, that individual will be able to be identified.

For a review of Access and Privacy basics for new employees please see GBJA-E-4.

Access to Information

The *Freedom of Information and Protection of Privacy Act* (FIPPA) provides a right of access to information in records held by public bodies. With certain exceptions, individuals may see and obtain copies of records in the custody of the Division.

If a request for records / personal information is received, contact the Access & Privacy Coordinator for guidance as to whether this information can be provided or alternatively if it needs to go through the formal FIPPA application process.

Pledge of Confidentiality for Employees / Volunteers / Others

The Division has a pledge of confidentiality that all employees and volunteers are required to acknowledge and sign. These forms are GBJA-E-1 and GBJA-E-3.

Employee Consent – Social Media

The Division has established an online presence using social media platforms to be used as communication tools. Photos and captions are only to be published with employee consent in line with the Employee Print and Digital Release Form (GBJA-E-2).

Privacy Breach Checklist

A privacy breach occurs when there is unauthorized handling of personal (health) information, such as access to or collection, use, disclosure or disposal of personal information. Such activity is “unauthorized” if it occurs in contravention of The Freedom of Information and Protection of Privacy Act (FIPPA) or the Personal Health Information Act (PHIA).

The most common breaches happen when personal information is stolen, lost or mistakenly disclosed.

Breaches or suspected breaches must be reported to the Access and Privacy Officer or Access and Privacy Coordinator for the Division, without delay. At this time a Privacy Breach Checklist will be used to evaluate the breach and determine next steps in the process (to be completed along with the Access and Privacy Coordinator).

At times, notifying individuals, Manitoba Ombudsman and/or law enforcement of the breach may be necessary but this will be determined by the Access and Privacy Officer.

Privacy Impact Assessment (PIA) Process

Under FIPPA and PHIA, public bodies and trustees have specific privacy obligations. These include how personal information can be collected, used, disclosed, and otherwise protected.

Protecting privacy is more than just upholding the law, it also involves taking a proactive approach to safeguarding the public's personal (health) information.

Risks to privacy can arise in many circumstances. Collecting excessive information, using intrusive means of collection, or obtaining sensitive details in unexpected circumstances all represent risks to the individual. The use or disclosure of that information, or its retention for an unduly long period, puts privacy at risk.

The PIA process assists in this proactive approach to evaluate a proposed or an existing program, service or activity in order to ensure personal information is safeguarded. The process examines potential impacts to privacy and considers reasonable measures to lessen these impacts.

Managers should consult with the Access and Privacy Coordinator when considering any new system, project, program, service or activity that may involve personal information to determine whether a PIA is necessary.