Data Security and Privacy - Best Practices

Table of Contents

INTRODUCTION

This document outlines privacy and security best practices for collecting and managing personal data. It also discusses the use of privacy impact assessments.

PRIVACY BEST PRACTICES FOR PERSONAL DATA COLLECTION

- Only collect the minimum amount of personal information needed. The less personal information collected, the less there is to manage and protect. Limit your data collection to the data points that are truly needed.
- Personal information should only be used for the purposes for which it was collected - before starting your data collection, determine what data you will need and how you will use it.
- Include a privacy notification when collecting personal information, to inform individuals why their information is being collected, under what authority it is collected (i.e. legislation), and a contact within your government that can answer questions. This should be included on forms that are used to collect information or provided to participants who are being interviewed verbally. Privacy notifications should be easily accessible/visible at the point where the data collection occurs. For example, if an individual is filling in a form, they should be able to find the notification on the form; if they are being interviewed, the notification should be handed to them at the start of the interview or prominently displayed during the interview.
- Review privacy communications for simple language, ensuring that your target audience can understand and evaluate the scope and intended use of data being collected.
- For larger data collection projects such as community surveys, keep the community informed about the purposes of the data collection and the data collection timetable. Consider creating information sheets, FAQs, posters, and website announcements to inform the community about the initiative.
- SGIGs conducting social well-being data analysis need to be mindful to ensure security measures applied to sensitive information are proportionate to the sensitivity of the information. Medical information about individuals is to be given the highest level of protection.

PIPEDA CASE #2003-226: The more sensitive the personal information the more protection it needs

PIPEDA case #2003-226 shows that the more sensitive personal information is, the more steps should be taken to protect it (see PIPEDA Case Summary #2003-226 Company's collection of medical information unnecessary; safeguards are inappropriate). In this case, an employee's medical reports were received in the company's office by fax machine located in an unlocked, accessible room. Among other things, the Privacy Commissioner considered PIPEDA Principle 4.7. Principle 4.7 states that personal information shall be protected by security safeguards appropriate to the sensitivity of the information. The Commissioner found employee medical reports were among the most sensitive medical information. The company violated Principle 4.7 in its use of the fax machine and not having strict safeguards to protect the medical reports.

SGIGs conducting social well-being data analysis need to be mindful to ensure security measures applied to sensitive information are proportionate to the sensitivity of the information. Medical information about individuals is to be given the highest level of protection. This protection principle is echoed in all privacy statutes across Canada. The Office of the Privacy Commissioner of Canada's Guidance Document: Access to Data For Health

Research outlines the legal provisions in BC that apply to the disclosure of personal information for health research. This includes the volume and sensitivity of personal information that may be disclosed. While SGIGs located outside of BC are not subject to this law, the principles contained in it may be helpful.

PRIVACY BEST PRACTICES FOR PERSONAL DATA MANAGEMENT

- Staff should only have access to personal information if it is required for them to perform their jobs.
- Provide training to staff and any third parties you are working with on your legislation, policies, and protocols related to privacy protection.
- Consider whether using anonymous data works for your project. Anonymous surveys allow you to collect data points while not collecting information that identifies an individual.
- If anonymity is not possible, consider de-identifying the data. This could be done by creating a random ID code number for each participant, and removing personal identifiers from the data set. The coded data can then be used for analysis and reporting, without the personal identifiers. The key to the code and the personal information is held by the data steward in a secure place with limited access. Chapter 5 of the Tri-Council Policy Statement: Ethical Conduct for Research Involving Humans (TCPS 2)(2018) has more information about de-identification.
- If you are storing data on the cloud, determine where the server is located and the physical route your data takes to reach the server. Data residing or routed outside of Canada may become subject to legislation of other countries (see the breakout box on **Data residency and the cloud**).

Data residency and the cloud

If you are storing data in the cloud (servers accessed over the internet), you must be aware of data residency issues. Data residency refers to the physical location of your data. If the server is located outside Canada, your data will be subject to the laws of the country it is located in. For example, data stored on a server in the United States may be accessed by the United States government under the USA PATRIOT Act. Ensure that you take data residency into consideration when considering cloud-based data storage options and email servers.

- Before collecting data, consider defining what types of data may be disclosed and what information will not to be disclosed. Will raw data sets be shared with anyone outside your organization? Can aggregate data, with personal identifiers removed, be disclosed while still maintaining individual privacy? Will the data analysis results be published in the public domain?
- Observe the principle that disclosure of personal information requires the consent of the individual that the personal information is about. If you plan to share or disclose personal information in any way (even if it is anonymized or aggregated), you need to inform your participants of this. If required, you can request participants to sign a consent form.
- Have employees and contractors with access to personal information sign a security and confidentiality agreement.

- Create a data retention and disposition policy to determine in advance how long the data will be kept and what happens to it at the end of its lifecycle. Will the raw data be destroyed after a number of years? Will it be kept permanently by your organization, or be transferred to an archive? These questions are important to consider in order to prevent a data breach and potential disputes about what to do with the data.

DATA SECURITY BEST PRACTICES[1]

- Consider any outside organizations that may have access to confidential data - for example, vendors and tech support staff for proprietary software systems; consultants or other third-party service providers; cloud or data centre service providers. Work with your IT staff to assess the potential risks and determine how to mitigate them.
- Use additive permissions when providing user access to a system.
- Where available, set defaults to deny access if a system or process fails.
- Ensure all access requests are verified for both digital and physical assets.
- Develop a comprehensive data security strategy.
- Encrypt your data when transferring to another party.
- Ensure your network anti-virus and firewall software are up to date.
- Use layered security. For paper records, this could mean keeping files in a locked cabinet inside a locked room, protected by a security alarm. For digital data, this could mean a combination of system user permissions, password protection, encryption and/or multi-factor authentication. Privacy Commissioners have held that using layered security is reasonable. Remember, the more sensitive the information the more stringent the security needs to be.
- Layered security is particularly important for data on a mobile storage device - ensure the device is physically secured, password protected, and encrypted to protect the personal information.
- Create a written security policy and include security measures in any research agreements with third parties.
- Ensure your servers are protected from physical damage, including fire and water damage.
- Encrypt your stored data, particularly if stored in the cloud or on any removable storage devices (e.g. USB key or portable hard drive).
- Isolate the network the data is stored on from the internet.
- Develop strong password policies.

[1] USGS. Data Management: Backup & Secure. https://www.usgs.gov/products/data-and-tools/data-management/backup-secure#backups

PRIVACY IMPACT ASSESSMENTS

Provincial, territorial and federal government bodies are required to conduct a Privacy Impact Assessment (PIA) when they are engaging in a new digital initiative, in order to confirm that they are in compliance with applicable privacy legislation. The purpose of a PIA is to identify and evaluate what potential risks there are to privacy protection for any new initiative, and to determine how best to mitigate those risks. Although SGIGs are not legally obligated to conduct PIAs for their own internal programs or projects, doing a basic assessment can be a useful exercise to ensure personal information is protected. It is best to do this during the planning phase of a data collection project, and to create a written report so that there is a record to refer to later when needed. The Tri-Council Policy Statement Ethical Conduct for Research Involving Humans TCPS2 2018, Article 5.3 has some helpful questions to consider for a PIA:

Type of information to be collected;

- Purpose for which the information will be used, and the purpose of any secondary use of personal information that is identifiable;
- Limits on the use, disclosure and retention of the information;
- Risks to participants should the security of the data be breached, including risks of re-identification of individuals;
- Appropriate security safeguards for the full life cycle of information;
- Any recording of observations (e.g., photographs, videos, sound recordings) in the research that may allow identification of particular participants;
- Anticipated uses of personal information from the research; and
- Any anticipated linkage of data gathered in the research with other data about participants.

If your SGIG has its own privacy statute, you can create a PIA template that references the important sections of that statute. If you have a research agreement with external researchers, add the results of the PIA to the research agreement so that the privacy issues are binding on the researchers. If you don't use a research agreement, or if the research is being done by the SGIG, create a written policy so that the privacy issues are addressed.

For more information about how PIAs are used for the Government of Canada, refer to the website for the Office of the Privacy Commissioner of Canada. Again, these guidelines are meant for federal government agencies, but they may provide some helpful guidance to SGIGs on how PIAs are used and what they can include.