



Office of the Information
and Privacy Commissioner

Suite 2460, 801 – 6th Ave. SW
Calgary, Alberta
T2P 3W2
Phone: (403) 297-2728
Fax: (403) 297-2711
Toll Free: 1-888-878-4044
Web: www.oipc.ab.ca
Email: generalinfo@oipc.ab.ca

Personal Information Protection Act (PIPA)
PIPA ADVISORY #8
IMPLEMENTING REASONABLE SAFEGUARDS

This Advisory was prepared to help organizations implement the *Personal Information Protection Act*, which came into effect on January 1, 2004. This document is an administrative tool intended to assist in understanding the Act. It is not intended as, nor is it a substitute for, legal advice. For the exact wording and interpretation of PIPA, please read the Act in its entirety. This Advisory is not binding on the Office of the Information and Privacy Commissioner of Alberta (OIPC).

Contents

Introduction
What are Reasonable Safeguards?
Policies
Personnel
Physical Safeguards
Technical Safeguards
Information Transmission
Outside the Office
Contracting
Breach Response
Other Resources

Introduction

Stories of lost and stolen laptops, hacked and lost databases, identity theft, various kinds of internet fraud and the general misuse of personal information are frequently reported by the media.

Many of these information security breaches involve personal information collected by private sector organizations in the course of carrying out their everyday business – retail purchase receipts with credit card numbers, expiry dates and customer signatures; mortgage documents; employee databases (sometimes with Social Insurance Numbers); credit applications; property rental applications; debt collection account files; customer databases, and so on.

Section 34 of the *Personal Information Protection Act* (“PIPA” or “the Act”) requires organizations to protect personal information in their custody or control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

This Advisory is intended to assist organizations in understanding the requirements of section 34 of PIPA and meeting their responsibilities under the Act. Proactive implementation of safeguards is the most effective way to protect individuals from the potential harm resulting from a personal information security breach.

This Advisory is **not** intended to be a comprehensive guide to information security. Organizations are encouraged to make use of their own internal expertise, and avail themselves of published resources and professional consultants as required.

What are Reasonable Safeguards?

Section 34 of PIPA requires organizations to make reasonable security arrangements to protect personal information in their custody or control. Organizations that have not made reasonable security arrangements will be in contravention of the Act, whether or not an incident occurs.

In determining what is “reasonable,” section 2 of PIPA identifies the standard to be applied as “what a reasonable person would consider appropriate in the circumstances.”

This standard acknowledges that reasonable “does not mean perfect.”¹ Personal information security breaches may still occur, even where reasonable safeguards have been implemented. Instead, the reasonableness standard requires organizations to take into account all relevant circumstances in determining what safeguards to implement.

¹ Investigation Report F06-01, Office of the Information and Privacy Commissioner, British Columbia, available online at www.oipc.bc.ca

Some factors that might be considered include:

1. **Reasonably foreseeable risk** – what are the risks that a reasonable person would contemplate and guard against?
2. **Likelihood of risk occurring** – some risks may be foreseeable, but are highly unlikely. A reasonable person will take greater care where there is a strong likelihood of a risk occurring. Organizations are not required to protect against every possible foreseeable risk. Some judgment is required to determine how realistic it is that a risk will occur.

Example: A Union employee exported information from the organization's member database for unauthorized purposes. Although the risk of unauthorized access by an employee had been foreseen, the Union could not have reasonably foreseen the extent and method of a data breach by a long-term employee who had legitimate access to personal information to perform his duties. The Union had appropriate policies and confidentiality agreements in place which the employee had understood, acknowledged, and then ignored. The Union was found to have implemented reasonable technical and administrative safeguards, despite the fact a breach occurred (OIPC Investigation Report #P2006-IR-004).

3. **Seriousness of harm** - harm refers to the impact associated with a risk occurring. The seriousness of harm may be very low if the personal information that is compromised is not very sensitive, or if only a few individuals are affected. Harm may be very serious if the personal information is sensitive medical or financial information that can be used to commit fraud or identity theft.² Organizations should also consider that they may be harmed by a personal information security breach through negative publicity, loss of customer business, or the time and money required to respond to a breach.

² For more information on assessing harm, see *Key Steps in Responding to Privacy Breaches*, Office of the Information and Privacy Commissioner, Alberta, available online at www.oipc.ab.ca.

4. **Cost of preventative measures** - the magnitude of a potential risk should be balanced by consideration of the cost of the measures needed to reduce or mitigate the risk. It may not be practical to implement extravagantly expensive and impractical safeguards to address minimal risks. On the other hand, where reasonable, affordable, and practical safeguards are available to combat foreseeable risks, they must normally be implemented.
5. **Established practice or custom** - another factor that may be considered in determining whether a safeguarding standard is reasonable, is whether that standard is consistent with established practices and customs of peer organizations, or a specific industry. Be aware, however, that compliance with established practice will not necessarily be deemed to be reasonable. Influencing factors include:
 - the longevity of the practice,
 - its universality,
 - the status and reputation of those who have implemented the standard (e.g. professionals, the type of industry),
 - the technical difficulty of implementing the safeguard (safeguards that are complex, scientific or highly technical may not be reasonable), and
 - whether the organization relied only on established practice without considering other precautions that may have been available.

Example: An organization's laptop computer with personal information of approximately 8,000 individuals was stolen from a vehicle. The organization relied on its employee to follow policies and not leave the laptop unattended in the vehicle. Information on the laptop was protected only by a log-on password. These safeguards were found to be insufficient. Instead, a combination of administrative, physical and technical safeguards - including encryption, which can be relatively inexpensive and has become a computing standard - would have been reasonable in the circumstances (OIPC Investigation Report #P2006-IR-005).

All of the above factors may be among an organization's considerations in determining what is "reasonable". However, remember that depending on the circumstances, the reasonable measures required to protect personal information may vary and even change over time.

Tip: In determining what reasonable safeguards to implement, an organization should conduct a risk assessment. A risk assessment is a systematic process of identifying, quantifying and prioritizing risks to the security of personal information.

The process involves identifying the organization's personal information assets, and assessing threats to that information as well as any vulnerabilities or weaknesses that might contribute to a risk occurring. A risk assessment will also consider the likelihood of a threat occurring, and the harm that might result. Based on the risk assessment, organizations can determine what safeguards should be implemented to eliminate or reduce risk.

A risk assessment may need to be repeated periodically to ensure that any changes in the environment, or new threats or vulnerabilities, are taken into account.

The remainder of this Advisory focuses on identifying some common safeguards to help reduce risk. This is not a comprehensive list of safeguards that may be implemented, nor does every organization have to implement each safeguard identified below. Instead, this information is provided to encourage organizations to consider and identify possible threats to the security of personal information in their custody or control, so that they can identify and implement reasonable safeguards to protect that information.

Policies

Section 6 of PIPA requires that organizations develop and follow policies and practices that allow the organization to meet its responsibilities under the Act. PIPA does not specify the content of policies, or the level of detail required. Organizations must assess their own

circumstances and develop appropriate policies and procedures as necessary.

When developing policies and procedures, remember that information privacy and security are not the same thing. An organization will need to address both privacy and security of personal information in order to effectively meet its responsibilities under PIPA.

Some suggestions to help meet the Act's requirements for protecting personal information are set out below.

- Develop and implement information **privacy** policies that provide rules governing the collection, use and disclosure of personal information. Policies should clearly state what personal information is collected, used and disclosed and for what purposes. Only personal information that is required to meet business purposes should be collected, used or disclosed. Access to personal information should be limited to authorized persons on a need-to-know basis to fulfill their job responsibilities.
- Develop and implement information **security** policies. A general umbrella policy stating the organization “protects personal information” will likely be insufficient. Instead, provide enough depth and detail so that policies are meaningful and address potential risks specific to your organization.

Example: If staff use laptops away from the workplace, it may be necessary to have a policy that specifically addresses personal information and computing equipment outside the workplace. If staff use email or fax to exchange personal information, it may be necessary to develop policies that address these practices.

- Communicate policies, including all changes and updates, to all staff and relevant external parties (e.g. contractors, service providers, agents, consultants, technical support, maintenance and support services). Ensure staff members are aware of their responsibilities arising from policies.
- Assign someone to ensure compliance with policies.
- Regularly review and update policies as necessary.

- Develop policies for retention and secure disposal of personal information, inclusive of all formats and media (paper, electronic, video, etc.). Policies should require that destruction of personal information is documented.
- Consider developing policies and procedures for conducting Privacy Impact Assessments (PIAs). A PIA is an in-depth, comprehensive review of an organization's programs, information systems, planned activities or new technologies and other trends to identify legislative requirements, assess potential risks, and develop solutions to mitigate risk. A PIA might examine how personal information is collected, used and disclosed, an organization's authority to engage in certain activities, the adequacy of existing or proposed safeguards, and other relevant matters. Although not mandatory under PIPA, completing a PIA may assist organizations in systematically assessing risks to personal information, and developing strategies or implementing safeguards to protect against those risks. PIA templates to assist with the process are available on the OIPC website at www.oipc.ab.ca.

Personnel

Many information security breaches occur because staff members are not aware of what is expected of them or, in some cases, as a result of intentional misuse of information. To minimize these kinds of risks, consider the following:

- Ensure that all job descriptions explain staff roles and responsibilities regarding personal information privacy and security.
- Conduct pre-employment screening checks where required. However, ensure that security checks and collection of information are directly related to job function.

Example: A software company conducted a credit check on an individual applying for a position as Administrative Assistant/Receptionist. The organization's purposes for collecting the credit information were to assess the applicant's suitability to handle cash, minimize credit card fraud, and validate employment history. An OIPC investigation found the

credit check was not reasonably required as the position only required management of a petty cash fund and there were other, less intrusive ways of verifying the applicant's abilities. Similarly, there were less intrusive ways to validate employment history and, as the applicant had applied for employment and not a credit card, there was no need for the organization to collect information to minimize the possibility of credit card fraud (OIPC Investigation Report #P2005-IR-008).

- Have staff review and sign-off information privacy and security policies. Review policies with staff on a regular basis.
- Have staff sign confidentiality agreements. Ensure agreements prohibit any further use of personal information after employment has ended.
- Provide information privacy and security education and training for staff at the time of hire, and regularly throughout the duration of employment.
- Ensure there are real consequences for staff who fail to comply with policies.
- When an individual's employment has ended, retrieve keys and/or access cards or tokens, revoke access privileges, change access codes, and ensure any personal information assets in the employee's possession have been returned to the organization.

Physical Safeguards

There are a number of safeguards that may be implemented to physically protect personal information assets.

- Ensure only authorized individuals have access to premises by controlling key distribution, and/or implementing features such as card swipes, or coded entry.
- Where appropriate, ensure access systems record the date and time premises are entered, and by whom.
- Install intruder detection systems.
- Ensure offices, storage rooms (on- and off-site), and file cabinets where personal information is stored are locked when not in use, and accessible only to authorized individuals.

Example: Cell phone contracts containing customer personal information were recovered in a police

investigation. The cell phone service dealer reported several previous incidents of staff theft. An OIPC investigation found that employee access to sensitive customer data was not restricted within the organization. Further, records containing personal information were stored in the accounting office and inventory storage areas, accessible to all of the organization's staff (OIPC Investigation Report #P2005-IR-003).

- Do not leave or store personal information in areas that are publicly accessible.
- Do not leave records containing personal information lying around unattended. Clear desks and regularly check photocopiers, printers, and fax machines.
- Direct computer screens so that they cannot be viewed by passersby.
- Locate equipment such as computer servers and fax machines in locked rooms, or away from common use areas.
- Ensure portable equipment (e.g. laptops, PDAs) is physically secured when not being transported (locked in cabinet, cabled to permanent furniture).
- Ensure any equipment that has been designated for re-use, disposal or surplus has been physically cleared of any personal information (e.g. computers, PDAs, laptops, copy machines, hard drives, diskettes, tapes, CD-ROMS, etc.). The same considerations apply when equipment is sent externally for maintenance or repair.
- Ensure hard copy records containing personal information are physically destroyed (shredded) when no longer required for legal or business purposes. If electronic storage devices (diskettes, tapes, CD-ROMs, hard drives) cannot be securely wiped, then they should be physically destroyed so that they cannot be read.

Example: Staff of a beauty supply organization disposed of customer personal information in a dumpster. The organization did not provide adequate direction regarding the confidential and secure disposal of records, and staff only tore the records by hand instead of shredding them (OIPC Investigation Report #P2006-IR-003).

- Provide fire extinguishers, smoke detectors, and sprinkler systems where personal information is stored.
- Install privacy partitions so that individuals providing personal information verbally cannot be overheard by others waiting in reception areas.
- Remember that new policies or additional safeguards may be required in exceptional circumstances such as when moving offices to a new location, or if records containing personal information are transported outside the office.

Example: A collection agency's debt collection account records were found by police in the possession of unauthorized individuals. The agency had recently moved to new premises and a number of gaps in the organization's security measures were exploited, resulting in a breach. Records containing personal information were left behind and not secured, and were at times accessible to unsupervised third parties; shredding bins were not secured; the premises alarm system was not always activated (OIPC Investigation Report #P2005-IR-002).

Technical Safeguards

Electronic environments introduce a number of security risks. Below are some technical safeguards to help eliminate and/or mitigate those risks.

- Restrict and control access to electronic files, directories, applications, databases, networks, etc. Access privileges should be based on job function and need-to-know. Regularly review and update staff access privileges.
- Ensure all users are assigned unique User IDs and passwords. Users should be authenticated every time they log on before access is granted.
- Require staff to use strong passwords (e.g. a minimum of 8 characters, use of both upper and lower case letters, numbers and symbols). Passwords should be unique, difficult to guess, changed regularly, and should not display on screen when being entered. Require staff to keep passwords confidential.

- Have computers log users out after a set period of inactivity. Implement screen savers and passwords when computers are left unattended. Ensure these features cannot be overridden by users.
- Protect networks with firewalls and anti-virus software. Monitor firewall logs to detect potential intruders. Regularly update anti-virus software.
- Initiate system audit capabilities so that access and use of electronic networks can be monitored.
- Implement user identification and strong authentication, encryption, network connection and access controls for all external connections with remote users.
- Regularly back-up electronic systems and develop and implement strict controls over back-up processes. Review backed-up information regularly to ensure it can be restored if necessary. Migrate information to new media as necessary. Provide secure off-site storage for back-ups.
- Completely delete or wipe all personal information no longer required for legal or business purposes from computer storage devices (diskettes, tapes, CD-ROMs, hard drives). If wiping is not possible, physically destroy the devices.

Example: A retail office supply store re-sold a computer that had been returned to the store. The new owner found personal information of the previous owner on the computer's hard drive. The organization contravened PIPA by failing to thoroughly eradicate the previous owner's personal information from the hard drive before reselling the computer (OIPC Investigation Report #P2006-IR-001).

- If your organization prints receipts for customer transactions, employ equipment that truncates or otherwise obscures credit card and debit card numbers on printouts.

**Information
Transmission**

Various means of transmitting personal information can put information at risk. Organizations may need to establish protocols for secure exchange or transmission of personal information. Expectations should be clearly communicated to all staff.

- Develop policies for transmitting personal information by fax. Policies should address whether faxing personal information is or is not acceptable and under what circumstances, the use of pre-programmed numbers, location of fax machines, calling ahead to ensure recipients are standing by, confirming receipt, mandatory use of fax cover sheets, etc.

Example: A collection agency faxed a Verification of Employment (VOE) form to a debtor’s place of employment. The fax was received on a non-confidential fax machine, and was collected by an unauthorized individual instead of the intended recipient. The organization did not have adequate policies or procedures in place to mitigate risks associated with faxing personal information (OIPC Investigation Report #P2006-IR-003).

- Develop policies for transmitting personal information by email. Policies should address whether email transmission is or is not acceptable and under what circumstances, potential risks and means to mitigate risk, encryption, blind “cc” features, etc.
- Implement standards for shipping personal information outside of the workplace e.g. require that files be transported in a sealed envelope marked “confidential”; use only trustworthy, bondable courier companies; document the shipment (date, time, contents, name of courier company), confirm receipt.
- Remind staff that the need for information privacy and security applies to verbal conversations as well. Avoid discussing personal information in public places, by cell phone, or anywhere conversations may be overheard.

**Outside
the Office**

It may be necessary for an organization to develop policies that specifically address the security of personal information outside the workplace - whether stored in paper files, or on laptops or other devices such as PDAs.

- Establish whether it is or is not acceptable to take personal information outside the workplace.

- Develop policies for the use of laptops and other equipment outside the office. For example, policies should limit or prohibit storage of personal information on laptops, and require user authentication and password controls as well as encryption. Laptops should never be left unattended, and should be stored securely when not in use. Additional controls might include equipment sign-out protocols, “kill switches” and remote equipment tracking mechanisms.
- Provide protocols for staff working at home or on the road. Hard copy and electronic personal information must be stored securely in home environments, and inaccessible to unauthorized persons. Mechanisms such as user authentication, encryption and/or virtual private networks should be in place to maintain security if networks will be accessed remotely.

Example: A laptop computer was stolen from the home of an employee of a health region. Although the laptop had a locking cable to secure it to a desk or table, this mechanism was not in force. The laptop had more health information than was required stored on its hard drive. The health information was not encrypted (OIPC Investigation Report #H2006-IR-002).

Contracting

Contracts between organizations and third party service providers should include provisions for ensuring appropriate information management and security practices by the third party (e.g. contractors, consultants, support service providers, etc.).

- Third parties should not have access to personal information without a signed contract/agreement in place.
- Contracts should limit the third party’s collection, use and disclosure of personal information to what is required to provide the contracted service.
- Third parties should be required to:
 - meet or exceed the organization’s security standards
 - have staff sign confidentiality (non-disclosure) agreements

- report information security breaches to the organization
 - have disaster recovery and system backup protocols in place
 - return personal information at the end of the contract
 - retain personal information according to the organization's records retention policy, or destroy it only as authorized by the organization.
- Contracts/agreements should include provisions allowing for the organization to audit/monitor the third party's compliance with contract provisions.

Breach Response

Despite having reasonable safeguards in place, information security breaches can still occur. The four key steps that should be taken in responding to a breach are³:

1. **Contain the breach** – recover the records, stop the unauthorized practice, revoke access, or shut down the system that was breached. Immediately inform the organization's Privacy Officer and/or person responsible for security. Notify the police if there is a possibility of theft or other criminal activity.
2. **Evaluate the risks associated with the breach** – identify the personal information that has been compromised (e.g. financial, health, etc.). Determine the cause and extent of the breach, including the number of individuals that may have been affected. Consider and assess how the information might be used and the possible harm resulting from the breach (e.g. fraud/identity theft, damage to reputations, loss of business, risk to public safety). What steps have been taken to minimize harm?
3. **Notify affected individuals where appropriate** – this is an important step where notification may help to avoid or mitigate harm to individuals. Consider notification where legislation or contractual provisions require it, where there is a

³ From *Key Steps in Responding to Privacy Breaches*, available online at www.oipc.ab.ca .

risk of identity theft or fraud, physical harm to an individual, or damage to reputations. Contact the OIPC for advice on assessing the need to notify affected individuals and what to include in the notification.

4. **Investigate the breach and develop an action plan** to prevent similar occurrences in the future – this may involve an audit of existing policies and safeguards and strategies to enhance security.

In responding to a breach, it is most important to act **immediately** in order to contain the breach and prevent the situation from deteriorating further, and to reduce the potential for harm to individuals or the organization.

Other Resources

For more information on **responding to information security breaches**, see *Key Steps in Responding to Privacy Breaches*, Office of the Information and Privacy Commissioner, Alberta, available online at www.oipc.ab.ca.

For more general information on **preventing privacy breaches**, see *Physicians and Security of Personal Information*, Office of the Information and Privacy Commissioner, British Columbia (www.oipc.bc.ca/pdfs/private/PhysicianSecurityofpersonalinformation.pdf).

For more information on **protecting personal information outside the office** see:

- *Protecting Personal Information Outside the Office*, Office of the Information and Privacy Commissioner, British Columbia ([www.oipc.bc.ca/pdfs/public/persinfooutsideoffice\(Feb2005\).pdf](http://www.oipc.bc.ca/pdfs/public/persinfooutsideoffice(Feb2005).pdf)).
- *Privacy and Confidentiality when Working Outside the Office*, Office of the Information and Privacy Commissioner, Ontario (www.ipc.on.ca/images/Resources/up-num_20.pdf).

For more information on safeguards when **faxing and/or emailing** personal information see:

- *Guidelines on Facsimile Transmission*, Office of the Information and Privacy Commissioner, Alberta (http://www.oipc.ab.ca/ims/client/upload/Guidelines_on_Facsimile_Transmission.pdf).
- *Faxing and Emailing Personal Information*, Office of the Information and Privacy Commissioner, British Columbia ([www.oipc.bc.ca/pdfs/public/fax-emailguidelines\(Feb2005\).pdf](http://www.oipc.bc.ca/pdfs/public/fax-emailguidelines(Feb2005).pdf)).
- *Faxing Personal Information*, Office of the Privacy Commissioner of Canada (www.privcom.gc.ca/fs-fi/02_05_d_04_e.asp).

For more information on **security in contracting** with third parties, see:

- *Model Contract Language*, Access and Privacy Branch, Alberta Government Services (www.psp.gov.ab.ca/index.cfm?page=resources/ModelContract.html).

Templates for completing a **Privacy Impact Assessment** (PIA) can be found on the website of the Alberta Information and Privacy Commissioner at www.oipc.ab.ca/pia/template.cfm. Although these templates specifically reference the *Health Information Act* they can be modified for PIPA organizations.

Additional information on PIPA and resources for complying with the Act are available on the websites of the Office of the Information and Privacy Commissioner, Alberta (www.oipc.ab.ca) as well as Alberta Government Services, Access and Privacy Branch (www.pipa.gov.ab.ca).

Visit the Queen's Printer website to view an online version of the Act (www.qp.gov.ab.ca).