Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

PRIVACYRIGHT fundamentals for business

Security safeguards

Today's webinar covers the security safeguards every private sector organization must have in place to protect the personal information it collects and uses.

PIPA requires organizations to protect personal information in its custody or control by making reasonable security arrangements to prevent unauthorized access, collection, use, disclosure, copying, modification or disposal.

What does this mean? Well, it means that organizations must ensure they have appropriate security controls in place to protect personal information from things like snooping, hacking, theft, loss, tampering, and copying of the information when not authorized. These types of incidents are referred to as breaches.

PIPA does not specify the particular security safeguards that must be used. How you protect the PI may change depending on the sensitivity of the PI you collect, the amount of PI, how it is stored and who needs to access it. So, whether you store PI electronically or on paper, you must have adequate security safeguards in place.

Safeguards to protect PI

Preventive, Detective, and Corrective safeguards can be used by an organization to protect PI…

The first, **preventive,** is put into place *before* an event occurs, to prevent the potential for a breach or other incident. Regular risk assessments and compliance monitoring can help you to identify risks and prevent breaches.

The second is **detective**…these are controls that help you identify a suspected breach. They also help you determine the scope of the breach.   Monitoring compliance with privacy policies and auditing the access to and use of information systems can help you to detect potential breaches.

And finally, there's **corrective**… these are additional safeguards that you put into place after a breach has been discovered to limit the potential harm, to recover PI that has been breached, and prevent this type of breach from happening again.

Security controls

There are also different types of security controls that your organization should consider as you develop your security safeguards.

There are administrative, physical, and technological security controls. Let's explore some examples of each type.

Administrative security controls are operational procedures and mechanisms, implemented primarily by staff or owners of an organization to ensure proper handling of PI, as opposed to through the use of automated systems or physical measures. Examples of administrative security controls include privacy policies, staff training, background checks, confidentiality agreements, breach response procedures, and compliance monitoring.

Check out our website for additional resources on these issues.

Let's take a closer look at some administrative controls.

Privacy policies explain *why* and *how* your organization handles PI. They help people understand *why* your organization collects PI, *how* the PI will be protected, and *who* people can contact if they have questions or concerns. Privacy policies are an important tool for staff to review, as they communicate your expectations about the secure handling of the PI they access or use in the course of their work day. Privacy policies are also useful in communicating with clients and customers, to ensure they understand how you will use and protect their PI. Documenting the security safeguards you employ is an important part of any privacy policy.

We've spoken in other webinars about the importance of providing privacy training to staff and ensuring they understand how to securely handle PI. Privacy training should be mandatory for all staff, contractors, service providers or anyone else who may access the PI your organization collects. Such training should be offered to any new staff or other individuals BEFORE they access any PI, and as a regular refresher.

Breach response protocols should be included in both the privacy policies and in staff training. Basically, protocols should document who your staff need to contact to report a suspected breach and expectations around:

- containing the breach,
- evaluating the risk of harm to individuals who may be affected,
- considerations for notifying affected individuals, and
- preventing future breaches.

Compliance monitoring is another administrative security measure. Organizations need to monitor the safeguards, training, and policies that are in place to ensure they are being utilized appropriately, to determine whether they are effective in protecting PI, and to see if anything needs to be updated.

Now, let’s take a look at physical security controls….

Physical security controls use *physical* restrictions to limit access to PI by unauthorized individuals. Examples of physical security controls include things like:

- fencing around a yard or building,
- locking doors to server rooms and areas of the business that contain paper records (including individuals office),
- locking cabinets within offices to control access to paper records or equipment
- clearing files and documents containing PI off desks at the end of the day,
- destroying computer hard drives that contain personal information before discarding them,
- digital card keys,
- anti-theft devices,
- alarm systems, or
- use of security personnel.

Physical security controls also include using appropriate methods to destroy personal information, such as cross-shredders for paper records. And, in the event of an emergency, mechanisms such as fire extinguishers and sprinkler systems are physical controls that can be used to protect PI.

OK, now let’s take a look at technological security controls….

Most people are familiar with this next category. **Technological security controls** are for protecting PI held in computer systems. Much of the PI businesses collect nowadays is electronic information, so having adequate technological security is really important. Examples of technological security controls include:

- use of unique electronic userIDs for each and every individual who needs to access the system

- use strong and secure passwords to make sure only authorized individuals have access to computer storage devices or to the network, and require that passwords be changed on a regular basis.

- use adequate encryption for storage and transmission, and definitely for any mobile device that is used to carry PI – like laptops, external hard drives, or USBs. It’s important to ensure your computer systems that hold PI are protected with firewalls, a*nti-virus software*, and intrusion detection;

- restrict access to personal information or ensure role-based access so employees can access only the PI they need to perform their job duties;

- deleting personal information once it is no longer needed and securely wiping all personal information from hard drives before you discard, sell or donate them; and finally,

- disaster recovery (such as off-site servers and performing regular back-ups).

Cloud storage

Remember that storing data in the Cloud or in proprietary software means there is likely disclosure of that personal information outside of Canada.

It is much more privacy protective to store personal information on a server located in Canada. That way, you can help prevent access by unauthorized third parties.

If you *do* store personal information with a service provider (whether they are inside or outside Canada), it is always preferable for you to encrypt or lock down the data before you give it to them.

Limiting time of retention

OK, a final point in addition to the security safeguards already mentioned, you should also limit the length of time you retain personal information.

With limited exceptions under PIPA, PI can only be used for the purposes for which it was originally collected. It should also only be kept for as long as is necessary to fulfil those purposes or related business or legal reasons.

Remember: PI used to make a decision that directly affects an individual *must* be retained for at least one year after you use it, so the individual has a reasonable opportunity to obtain access to it.

When disposing of PI, organizations need to ensure it is securely destroyed.
We talked earlier about devices like cross-shredders to help you securely destroy paper records. The same goes for PI held electronically. You should either erase or anonymize any PI no longer needed for the purpose for which it was collected.

For an example, let’s look at application materials you’d typically collect during a hiring process:

If you requested applicants to provide a resume or to complete an application form, you must keep the documents for at least one year, presuming you used the PI to make a decision about whether to consider them for the position.

What if you received a resume, but didn't look at it?
Well, for unsolicited resumes, if you don't look at them, you don't need to keep them at all and can securely destroy or delete any copies.

BUT if you use the information (or hold onto the resume for possible future use) you're responsible for protecting the PI included in the documents and for responding to an individual's enquiries about how their PI has been used or disclosed.

Once the PI in the document is no longer needed, and after a year has passed from when it was used to make a decision that affects the individual (if applicable), you should securely destroy or delete it.

So, there you have it – an overview of security safeguards. Security safeguards, like other aspects of a privacy management program, can be scalable to your organization and for the types of PI you collect.

More sensitive PI needs to be protected with more extensive controls.

Key considerations

Remember, when building or updating your security safeguards, consider:

- The sensitivity of the PI you collect
- The amount of PI you collect
- The format the PI is kept in (such as electronic or paper records)
- And lastly, who needs to have access to each aspect of PI

Make sure you regularly review your organization's security safeguards to ensure they are up-to-date and to address any vulnerabilities.