Office of the Information & Privacy Commissioner for British Columbia

Protecting privacy. Promoting transparency.

PRIVACYRIGHT fundamentals for business

Basic obligations of PIPA

Today's webinar covers **ten basic obligations of private organizations under PIPA**.

So what exactly is personal information, also known as PI? PI describes any information that can be used to identify someone - either by itself or in combination with other information.

Everyone's personal information is protected under PIPA – yours, your employees', customers', and contractors'.

One thing to keep in mind: PI DOES NOT include business contact information or work product information.

Some specific examples of PI are a person's:

- name,
- address,
- gender,
- image,
- education,
- income,
- financial information,
- medical and genetic information,
- date of birth,
- drivers' license number, and
- employment history.

PIPA outlines how private organizations must handle this PI.

The obligations under PIPA follow the same basic privacy principles that are recognized internationally and found in most privacy legislation around the world.
So let's get started breaking this privacy law down into the ten privacy principles!

The very first privacy principle is that of accountability.

Why is accountability so important? Well, as an organization, you are legally responsible for any PI that you collect, use, and disclose.

But don't worry, there are a number of actions you can take to be accountable.

The first thing you can do is begin to develop a privacy management program within your organization. This can be initiated by having a privacy officer and drafting privacy policies.

A privacy officer is the person responsible for developing your program and maintaining ensuring privacy policies are up to date, and monitoring to see whether that the agreed upon practices are actually in use. The contact information for the privacy officer must be easily available for both staff and the public, and should be included in your organization's privacy policy.

Organizations in BC must develop and follow policies and practices relating to privacy management for the organization to meet its obligations under PIPA. Policies must include processes for handling personal information. They should also explain what to do if someone requests a copy of their own PI from your organization (which you have to provide), or what to do if someone has a complaint about how your business is managing PI.
These policies should also be available for the public to see, for instance, on your organizations website.

Ok, let's move on to principle number two. The second privacy principle is to identify the purpose of your organization's collection, use, and disclosure of PI. PIPA provides individuals with the right to know what personal information is being collected, used or disclosed by your business and for what purposes. Before or at the time you collect personal information, explain why you're collecting it, and how you intend to use this information.

Use the 'Reasonable Person Test' to evaluate the purpose of the collection, use, and disclosure of PI by your organization. Ok, so what does that mean?

The reasonable person test considers the nature of the information collected, the purposes and circumstances surrounding the collection and the use of the information, and how the organization handles the information. Think about whether a reasonable person with no special interest would consider the way your business handles personal information appropriate.

Let's take a look at the third privacy principle - obtaining consent! PIPA is a consent-based statue, so your organization almost always needs an individual's consent whenever you collect, use, or disclose their PI. There are different types of consent, depending on the circumstances.

The first type of consent is "express consent". This is when a business provides notification so the person is fully aware of how and why their PI is being collected and then willingly agrees to this action.

Express consent can either be verbal and written. For instance, someone can sign their name or verbally answer 'yes' to a clear question. Onto the second form of consent - "implied consent".

Implied consent is given in the same written or verbal form as express consent but notification is not needed. This is because the purpose for collecting this personal information should be obvious and not need any further explanation for the person to be fully informed. For instance, a person handing over their medical card to the doctor's receptionist would be giving implied consent for the receptionist to charge the health insurance provider for the person's visit.

The third type of consent is "opt-out consent". This requires your organization to notify a person of the intended use of their PI and then give them the option to not participate by un-checking an agreement box. So if you read a terms of service agreement that has an automatically selected 'I agree' checkbox and you don't un-check the box - that would be considered opt-out consent. The difference between "opt-out consent" and "express consent" is that, with opt-out consent, the default is to consent to the collection.

This form of consent should only be used as a last resort, as the other two forms of consent are more straightforward for the consenting person. So there are the three main types of consent. Although each is obtained differently, they actually have some important rules in common.

For instance, when determining which type of consent to use, an organization must complete the reasonable person test that we just talked about earlier in this webinar – would a reasonable person consider how you obtained consent to be appropriate in the circumstances?

Your organization must also make sure that your chosen consent style is always used in a clear and transparent way.

An organization must never obtain consent in a deceptive way or provide false or misleading information in order to gain consent. This would actually be an offence under PIPA and your organization could be fined.

In most circumstances, people also have the right to withdraw their consent at any time.

If someone does withdraw consent, this means that you must stop using their PI.

Alright, onto the fourth privacy principle. This one is pretty simple, but crucial. You should collect ONLY the minimum amount of PI required to achieve the purpose that you stated. Remember the reasonable person test. Think about whether a reasonable person with no special interest would consider the collection of personal information appropriate.

And now the fifth privacy obligation – we're halfway there!

Similar to limiting collection, privacy principle 5 requires your organization to limit use and disclosure of PI to the original purpose that was explained to the person whose personal information you collected. This means that if your business wants to use PI for a new purpose, you need to go back and do the reasonable person test to determine if this new use is appropriate. Then you must obtain consent from the individual for the new uses you propose.

AND make sure to keep PI only as long as necessary to fulfill this identified purpose.

However, if the PI is used to make a decision about a person, such as not offering them a job with your organization, you must keep the information for one full year. This is so that person can request access to their PI after the decision has been made.

As soon as PI is no longer needed for any legal or business reason, it must be destroyed or anonymized. All of these steps help limit the collection of PI to its original stated purpose.

Ok, let's move on to number six. This sixth obligation requires your organization make a reasonable effort to ensure the PI you collect is accurate and complete.

Under PIPA, anyone can ask for a correction to their PI. If your organization does not make the correction, you must annotate the personal information noting that a correction was requested but not made.

Onto number 7! Okay, so you're required under law to take "reasonable security measures." What does this mean? Well you need to implement security safeguards to ensure that you and your staff or contractors handle personal information properly and to prevent privacy breaches. There are many different types of security safeguards, and deciding which one to use should be based on the sensitivity of specific PI.

Some easily implemented safeguards are: Limiting access to PI to protect from unauthorized internal and external access. Some of your employees may not need to have access to all aspects of personal information of your clients or customers.

An example of this is implementing a role-based form of access for employees.

This safeguard helps to ensure information is shared on a "need to know" basis. Another security safeguard is making sure all members of your organization know how to properly and confidentially handle personal information and the steps required for dealing with a breach.

The protocol for a privacy breach comes in four simple steps. First, contain the breach by stopping the unauthorized practice, recovering any possible records, and then changing access codes or passwords and/or correcting other weaknesses that lead to the privacy breach.

Next, evaluate the risk by identifying the type and sensitivity of the compromised PI, the cause and extent of the breach, how many people are affected, and if any future harms (such as identity theft) could come from this privacy breach.

Then, determine whether notification is necessary to those who's PI has been affected. You should notify the individuals if it will help reduce the harm of the breach. Other people who may need notification are our office, the police or RCMP.

Your organization should also consider reporting the incident to our office for help with managing the privacy breach. We can provide a number of tools and resources for you, including specific advice on your organization's privacy breach.

And finally, develop prevention strategies for the future, to make sure it doesn't happen again. Review and update your privacy management program and ensure staff are provided regular privacy training and refresher training.

Onto privacy principle number eight! The eighth principle is openness. Be open about your information management policies and procedures. Upon request, you need to make the following information available for any clients, customers or employees:

- the title and contact information of your designated privacy officer,
- the process an individual can follow to access their own PI, and
- information on your policies and practices surrounding personal information.

We're almost through all ten PIPA obligations!

Number nine is to provide customers, clients and employees with access to their own PI.

Any person is entitled to a copy of all of the PI that your organization has on them.

So, for example, if you're using video surveillance, you must be able to supply anyone who makes an access request all clips containing their image, while also protecting the privacy of others in the footage. This means blurring or using other technology to ensure the other individuals cannot be identified.

Alright, here we are at the final privacy principle! The 10th principle refers to the right of any person to question and challenge an organization's compliance with the Personal Information Protection Act.

Organizations are required by PIPA to develop a process to respond to such complaints. Remember also that the Openness principle pointed to being able to share this information with individuals who request is. This can be most easily accomplished by having written complaint handling policies and procedures that anyone can access.

Organizations should investigate and attempt to resolve all complaints received.

When responding to a complaint, you should also inform the person about other avenues to voice their concerns, such as reaching out to our office.