Privacy Management Programs

Today's webinar covers the ten steps involved with developing a privacy management program.

But first, what exactly is a privacy management program? Well, it's like a business plan, but for privacy management. Privacy management programs are about what goes on 'behind the scenes,' to ensure that the personal information your organization collects is protected.

A privacy management program can help your organization comply with PIPA. It can also help you identify weaknesses, reduce privacy risks, and ensure that your employees know what is expected of them.

Whether you are a non-profit, doctor's office, charity, trade union, business, or any other type of private organization that collects or uses personal information – your organization should have a privacy management program in place.

Today, we focus on 10 steps to follow when building a privacy management program. We will discuss each of these steps throughout this webinar, but let's take a quick look at them before we begin.

1. Buy-in from the top
2. Privacy officer
3. Reporting structures
4. Personal information inventory
5. Policies
6. Risk Assessment
7. Training
8. Breach response
9. Service provider management and finally,
10. Review and revise

Buy-in from the top

The very first step is to make sure you have organizational commitment for your privacy management program. This means having buy-in from the top, designating and supporting a privacy officer, and establishing reporting mechanisms.

It's important for senior management to commit to and support the development of the privacy management program. Buy-in from the top is not only the key to a successful privacy management program, it's essential for a privacy respectful culture.

How do executives demonstrate commitment and support? They make sure resources – including staff and equipment – are available to develop and maintain the privacy management program.

Privacy officer

This leads into our next step: to designate someone as the office's "privacy officer".

The privacy officer can be anyone in your organization who is able to take on the privacy management responsibilities. In larger organizations, the privacy officer may need support staff, while in smaller businesses, one person may be all that's needed to manage the duties. No matter the size of your privacy team, it's important that there are adequate supports and resources. So what are some of the privacy officer's responsibilities or duties? First, the privacy officer is responsible for ensuring the organization's general compliance with PIPA …

The privacy officer is also responsible for the design of your privacy management program…

This includes keeping the privacy management program up to date and making ongoing adjustments. In addition, privacy officers are typically responsible for:

- creating privacy policies,
- providing employee training,
- representing the organization during OIPC investigations, and
- advocating for privacy across the organization.

Your privacy officer should also support other staff members and foster an overall culture of privacy.

Reporting structures

The third step in your privacy management program is to make sure your organization has reporting mechanisms in place.

What do we mean by reporting mechanisms? Well, your organization needs an internal reporting structure so the right people know how the privacy management program is structured and whether it is functioning as expected.

Personal information inventory

The fourth step is to develop a personal information inventory.

A "PI inventory" will help your organization keep track of the PI you collect. It will also help you to establish retention needs and to determine if you still need to collect each type of PI. With a

PI inventory in place, you'll also be able to quickly identify relevant PI if someone requests their own information or to determine what PI may have been affected in the event of a breach. The PI inventory is typically only available to designated individuals within your organization.

You can design your PI inventory in a way that makes sense for your organization. What should organizations typically include? Well, first of all, ask yourself *what* type of information does your organization collect?

Types of PI include contact information (such as names, emails, phone numbers, addresses), payment information (such as credit card numbers), purchase history (such as details of the products or services a client has obtained from your organization in the past. Do not include any actual PI in this inventory; instead, just record the **type** of personal information that your organization collects.

Next, ask yourself *who* you are collecting each type of PI from. This could be anyone from an employee, volunteer, client, contractor… really anyone who interacts with your organization!

It's also important to track *why* you collect these types of PI. When you document your reasons for collection, and how the PI will be used or disclosed, you will be better able to make future decisions about the PI.

Organizations should also document the sensitivity of the collected PI. This will help you to determine the kinds of security safeguards you'll need to have in place to protect the PI.

Finally, you should document where you are holding the PI. This can be an electronic system or program or the physical location where the records are stored. If you have a breach, this information will help you quickly determine what PI may have been accessed. It will also help you locate PI if you get a request from an individual for their own information.

Once you have recorded all of this information, your PI inventory should be easy for your privacy officer to maintain.

Policies

Next comes the fifth step in the privacy management program process – drafting a privacy policy! So what exactly is a privacy policy? A privacy policy explains your organization's responsibilities for handling the PI you collect and use. It will help others understand why your organization collects PI – and how the PI will be protected. You can also use your privacy policy to train your staff.

When writing your privacy policy, remember to use plain language. PIPA requires privacy policies be available upon request – so making your privacy policy publicly accessible on your

website is an easy way to accomplish this! Check our website for a separate webinar dedicated to privacy policies.

Risk Assessment

We are now more than halfway there! Let's take a look at step six - 'risk assessment'.

Risk assessment involves looking at the PI your organization collects and evaluating whether you have sufficient safeguards in place to protect it. You're probably already monitoring the security of the information you collect. But there may be new risks that you didn't think about when you first started collecting the PI. Check our website for a separate webinar that discusses risk assessment and for now, remember that risk assessment should be documented as an ongoing activity in your privacy management program.

Training

The next step in your privacy management program is one we have already talked about: training.

When it comes to privacy management, it's important to educate all of your staff and volunteers about your organization's responsibilities and expectations. Every member of your organization should know how to collect and handle PI. Education and training contribute to a privacy-positive environment!

Breach response

Moving on to step 8 – breach response.

Ok, so what exactly is a privacy breach? A privacy breach is any incident involving the unauthorized access of individual's personal information. Protecting PI means protecting against breaches. Most privacy breaches happen when the PI of customers, patients, clients, or employees is stolen, lost, or mistakenly disclosed.

Accidents happen. This is why it is so important to have a documented process that staff can follow to report suspected breaches when they occur. How and when do you want staff to report? The OIPC has guidance available to walk you through the key steps of responding to a suspected breach. Have a look at these documents for ideas when drafting your own breach response protocol. And make sure to check out our webinar on this topic.

Service provider management

Ok, so now that you have a privacy policy, your security safeguards are in place, and you have trained your staff and volunteers on how to protect PI and what to do in the event of a breach… the next step is to ensure your service providers are also aware of these expectations.

If you have hired service providers or contractors, you need to make sure they understand the expectations for privacy and security of that PI. These expectations should be communicated in contracts, discussions with the service provider or contractor, or perhaps even through formal training.

Review and revise

Ok, we made it. The final step for your privacy management program is 'review and revise'.

Now that you've built your privacy management program, the final step is to plan for a regular review of your program, so you can change anything that isn't working.

On at least an annual basis, you should:

1. review and update the personal information inventory;
2. review and revise your policies to ensure they're still current;
3. assess risks to the security of the PI your organization collects and evaluate whether your security controls are functioning effectively – if not make any necessary revisions; and
4. review the training program to see if it's still current. Ensure that all staff participate in regular training.

Remember, this is your program, and you can customize it to meet your unique needs. Think of your privacy management program as a living document. Make changes when necessary to ensure your program continues to meet your needs.