Using and disclosing personal information

Today's webinar covers the difference between using and disclosing personal information.

You might be wondering what the difference is between using personal information and disclosing personal information. *Using* PI usually means using it *internally* to carry out your organization's purpose for collecting the information. *Disclosing* PI means showing, sending or giving some other organization, government, or individual the PI in question.

Using PI within your organization should be limited. Ensure that PI, especially sensitive information, is accessible **only** on a need-to-know basis. Implementing this type of "role-based access" is the best way to ensure that employees can only view what they **need to know** to perform their work duties.

For example, staff members who don't process invoices likely have no need to view a client's billing information such as their credit card number. Note that both paper and electronic records need to be considered when limiting access to PI within your organization.

PIPA requires organizations to take reasonable security measures to protect personal information. This includes unauthorized access from people ***inside*** as well as **outside** your organization.

Your organization should have written policies or procedures that deal with how others can request access to the PI your business collects. This helps those who are responsible for the PI decide whether or not to grant access for its disclosure.

Under PIPA, you must have a process in place for individuals to request access to their own PI, or to make complaints if they have concerns about your organization's handling of their PI.

We've talked about using and sharing PI within your organization. Now let's move on to disclosing PI.

Disclosing personal information

There are actually very few occasions when an organization can disclose or share the PI they collect from clients, customers, volunteers, employees or others *outside* of their own organization.

Typically, you can only disclose PI for purposes that a reasonable person would consider appropriate in the circumstances.

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.

Your organization must also have the individual's consent to disclose their PI. And that consent is limited: if you create a new purpose for disclosure, you need to ask for consent again.

When *can* organizations disclose PI to third parties?

Remember when we said that organizations **can** disclose PI without consent in certain circumstances?

Here are some examples of people who may be authorized to access an individual's PI without consent:

1. Authorized employees who need certain types of PI to perform their job may access and use the information within your organization;
2. Other organizations who need to access the PI in order to provide contracted services to your organization;
3. Collections agencies contracted by the organization to collect amounts owed;
4. Legal representatives for the organization or the individual whom the PI is about;
5. Government agencies, if authorized to collect the PI under their own legislation;
6. Our office, the OIPC; and
7. Law enforcement.

Organizations can also disclose employee PI without consent if the disclosure is again, **reasonable,** for the purposes of establishing, managing or terminating the employment relationship. For example, it would be appropriate for an organization to disclose an employee's social insurance number to the Canada Revenue Agency because this is a necessary component of managing an employment relationship.

As I mentioned, before you disclose any personal information to others outside of your organization, you must ensure that you have the authority under PIPA to do so.

Also, if a contractor discloses PI in way that is not authorized, your organization will be responsible for managing the breach.

This is why it's **so** important to set out requirements and expectations for government bodies, collection agencies, or other contracted service providers to safeguard your organization's PI.

By doing so, you'll ensure that other organizations and contractors have a thorough understanding of the requirement to protect the PI they receive from your organization.

Information Sharing Agreements

An agreement like a contract or Information Sharing Agreement that outlines the terms and conditions for sharing PI is the best way to accomplish this.

These documents can be prepared for one-time or regular exchanges of PI. They outline the roles and responsibilities for each party and guide the parties to the contract or agreement, so they know when and how the sharing of PI can occur.

Make sure to include detailed information about the intended exchange of PI, including:

- how and when PI will be shared,
- limits on use and any further disclosure,
- required safeguards,
- how and when to either return or destroy PI,
- processes for reporting and managing any suspected breach, and
- how your organization will monitor compliance with the ISA.

Check out our guidance document on information sharing agreements for more information.