SPOTLIGHT ON STANDARD 12: PRIVACY AND CONFIDENTIALITY

Case Study #1

Reporting a privacy breach

You are a Licensed Optician and the manager of an optical store. The store's receptionist reports to you that the computer system and client records have become inaccessible due to what appears to be a cyber security breach.

A cyber security breach is considered a privacy breach. In the event of such a breach, you must take steps to ensure that risk is managed.

You review the Office of the Information & Privacy Commissioner's Privacy Breach Checklist. The checklist helps you to identify whether you are required to report the breach to the Office of the Information & Privacy Commissioner in order to comply with the CHCPBC Optician Standard's of Practice. Additionally, the checklist helps you to:

1. Complete a risk evaluation.
2. Identify who must be notified of the breach.
3. Identify how to prevent further risk of harm.

You determine that a large number of client records containing personal information have been compromised and that some of the personal information is sensitive. Therefore, you determine that you must report the breach to the Office of the Information & Privacy Commissioner and request their assistance. You review information on reporting a privacy breach and complete the Online Privacy Breach Report Form. You use the information you've collected to complete the Privacy Breach Checklist and file your report.

What criteria from *Standard 12: Privacy and Confidentiality* were considered in Case Study #1?

12.1 Adhere to all relevant privacy and confidentiality legislation and regulatory requirements.

12.8 Report privacy breaches to the Office of the Information and Privacy Commissioner for British Columbia (OIPC) to ensure management and mitigation of risk.

Case Study # 2
Considerations for retiring or sale of a business

You are a Licensed Optician who is planning on selling your optical business. You review what responsibilities you have regarding your business's client records and make an action plan for how to manage them.

Through your review of the *Personal Information Protection Act* (PIPA), you determine that you may disclose personal information without consent in the sale of your business, as long as the following conditions are met:

1. The new business owner will maintain the store as an optical business and provide opticianry services to the public. (The personal information on file may only be used or disclosed for the purposes for which it was collected.)
2. All clients whose personal information will be disclosed must be notified that the optical business will have a new owner and that their records will be transferred to a new optician.

Your hope is that your store will remain an optical business, but you make a back-up plan detailing what you would do with client files if the new owner chose to take the business in a different direction. In that case, you would need to transfer the files to another optician or securely store the files. You decide that you would transfer the files to an optician who works at an optical store a block away from your business. (Your clients' personal information can be transferred to another optical business if that business will be providing opticianry services on behalf of your business after the sale of your business is completed.) The applicable clients would need to be notified of the transfer and of where their records were going. A client could also choose to collect their record to provide to a new optician of their choosing, instead of having their file transferred.

Your action plan also details what to do with older or "inactive" client records. CHCPBC requires you to keep client records for a minimum of three years and recommends you keep them for seven. This is counted from the date of the last entry in the record or the date when the client was last seen by you.

You will have to sort through your client files to determine which ones should stay/be transferred and which ones must be destroyed.

Section 20 of PIPA dictates the requirements for disclosing personal information in a business transaction. This section is the best place to start

when creating an action plan related to the sale of your business to another optician or to a person who intends to maintain the business as an optical store. Additionally, you may wish to refer to A Guide to BC's Personal Information Protection Act for Businesses and Organizations, prepared by the Office of the Information & Privacy Commissioner. Guideline 7 contains a detailed outline, explanation, and tips for best practices in a business transaction, while Guideline 10 contains rules for protection and retention of personal information.

Section 18(2) of PIPA allows for the disclosure of personal information to another organization if that organization will use the information for the purpose for which it was originally collected and will assist in carrying out work on behalf of the original organization. Section 18(2) provides guidance for selling your business to a non-optician or a person who does not intend to use the space as an optical store.

What criteria from *Standard 12: Privacy and Confidentiality* were considered in Case Study #2?

12.1 Adhere to all relevant privacy and confidentiality legislation and regulatory requirements.

12.4 Store, transfer, and dispose of client records in a manner that protects client confidentiality, except in circumstances specified by law.

Some requirements from *Standard 14: Record Keeping and Billing* also apply. Specifically:

14.9 Retain all client records for a mandatory minimum of three years and a recommended maximum of seven years from date of last entry.

14.10 Destroy records containing personal or health information in a secure manner.

14.11 Upon retirement, sale of the practice, or extended closure of the practice, notify CHCPBC of the change, and ensure that files are not abandoned and are securely transferred in accordance with applicable privacy legislation.

14.12 During an extended closure, take reasonable steps to ensure that clients can access their records.

Case Study #3
Signed consent and transfer of records

You receive a call from someone who says they are an optician in a small town in BC. They advise you that one of your former clients has moved to this town and would like their client record transferred for continuity of care. You ask them to provide you with their name and business details, as well as the client's name. You also advise that you will require a written consent form from your former client before you can send them the client record. You confirm the optician's licence is up to date on the CHCPBC website by using the public directory.

The information in the client record belongs to the client, and you have an obligation to provide that information in a timely manner when requested. Once the signed consent form is received through an encrypted email, you prepare a copy of the client record. Then, you contact the requester to find out their preference for receiving the client's personal information in a secure manner. Though the security of personal information is never guaranteed, you offer to use courier, mail, or an encrypted email file, as all of these options are generally secure.

You record the date of the transfer and the name and business details of the requesting optician/office on the original copy of the client record still in your possession. You add the signed consent form to the record as well. Even though the client has moved, you must maintain a copy of the client record for a minimum of three years after the date of the last entry.

The client's new optician receives the client record, ensuring that the information remains secure and that unauthorized individuals do not have access to it. They review the information with the client and make the necessary changes and updates before proceeding with any services.

Section 6 of the Personal Information Protection Act (PIPA) dictates how personal information can be collected, used, and disclosed with an individual's consent. Meanwhile, Section 18 of PIPA explains how information can be disclosed without consent. This case scenario requires client consent for disclosure based on the requirements outlined in PIPA.

What criteria from *Standard 12: Privacy and Confidentiality* were considered in Case Study #3?

12.1 Adhere to all relevant privacy and confidentiality legislation and regulatory requirements.

12.2 Perform services in a manner with consideration for client confidentiality.

12.4 Store, transfer, and dispose of client records in a manner that protects client confidentiality, except in circumstances specified by law.

12.5 Obtain client consent before collecting, using, and/or disclosing confidential information to parties outside of the client's circle of care, except in circumstances specified by law.

12.7 Ensure that client personal and health information is accurate, complete, and up to date.

Some requirements from *Standard 14: Record Keeping and Billing* also apply. Specifically:

14.2 Ensure that all records are updated to reflect new information as it becomes available.

14.3 Comply with all privacy legislation and standards related to the collection of, access to, and disclosure of records.

14.5 Maintain client records in a manner that enables timely access, as required, by the client or by an authorized CHCPBC inspector.

14.6 Provide the client with reasonable access to the information maintained about them in their client record.

14.7 Upon client request, facilitate the timely transfer of the client record to another regulated health care professional, in accordance with relevant legislation.

Case Study #4
Circle of care

You are a Licensed Optician who is certified to perform independent automated refractions in BC. Your client has just filled out *Form 1B: Sight Testing – Client History & Eligibility*, and you are reviewing the form with them in your refraction room—a private area of the store where you can maintain client confidentiality. This client's medical history is quite complex.

You decide to step out and consult with a co-worker who is more experienced in assessing client eligibility.

When you go back into the main part of the store, you find your co-worker at the front desk; their client is looking at frames nearby. You do not detail your client's medical history to your co-worker in front of their client, as this could be a disclosure of personal medical information. Instead, you ask that the co-worker briefly accompany you to the private area of the store. They advise their client that they will be back shortly, and they signal to another optician on the floor who can assist in the meantime.

Your co-worker evaluates your client's *Form B* and determines that you are required to recommend an eye health examination.

Even though it was inappropriate to discuss your client's medical history in front of another client, it was okay to share it with your co-worker. Why is this?

Your co-worker is within your client's "circle of care," just as you are. Within that circle, client information can be shared with the client's *implicit consent*. Put another way: by explicitly consenting to share their information with *you*, the client implicitly consented to that information being shared with your co-worker, who is assisting in their care. As long as the purpose of sharing the information would be considered obvious to a reasonable person, and the client has provided the information to the organization for that purpose, implicit consent applies. Section 8 of PIPA provides a framework for implicit consent.

This case study illustrates one aspect of the circle of care that we often see among eyecare professionals and how information can be shared amongst that circle for the client's benefit.

What criteria from *Standard 12: Privacy and Confidentiality* were considered in Case Study #4?

12.1 Adhere to all relevant privacy and confidentiality legislation and regulatory requirements.

12.2 Perform services in a manner with consideration for client confidentiality.

12.3 Conduct assessments, treatments, conversations, and consultations in a manner that preserves client confidentiality and privacy.

For more information on the standards, please review the Standards of Practice page on our website.