

On May 22, 2020 the Provincial Health Officer (PHO) updated an [order](#) that food and drink establishments must, if already collecting information from patrons to make reservations or to seat them, retain contact information for one member of every party of patrons for 30 days. The purpose of collection is for the local medical health officer to conduct contact tracing if someone who visited the establishment is diagnosed with COVID-19.

The purpose of this guide is to assist establishments subject to this order with compliance with this requirement in a manner that also protects patrons' privacy under BC's [Personal Information Protection Act](#) (PIPA). For more information about PIPA, see our guide [here](#).

Collected personal information is valuable, and can be used for many purposes. Because of its value, this information is susceptible to being stolen or misused. Under [s. 34](#) of PIPA, organizations must protect personal information by making reasonable security arrangements to prevent unauthorized access or similar risks. Below are some tips to help you securely collect, store, and dispose of personal information from patrons.

Explain to customers why you are collecting their contact information

At the time of collecting a patron's contact information, clearly explain what information you are collecting and why. Reference the PHO order (it would be helpful to have a copy on hand if a customer would like to see it).

Only collect the minimum amount of personal information necessary

The purpose of collection is to notify individuals if they have come into contact with someone diagnosed with COVID-19. Therefore, name, phone number or email, and date of visit from one member of the party should be sufficient. Do not collect a patron's physical address or other contact information such as where they work.

Do not use or disclose the collected information other than to provide to the PHO upon request

Do not use the collected information for other purposes, such as marketing or analytics. Further, do not provide the collected information to anyone other than the PHO upon request or as authorized in certain circumstances under BC's PIPA. Consult PIPA or [contact us](#) if you want help deciding whether PIPA authorizes your organization to make a disclosure.

If you share the collected information with the PHO, keep a record of the transaction

If the information is requested by the PHO, keep a record of what information you share. Under [s. 23](#) of PIPA, individuals have a right to ask organizations who the organization has disclosed their personal information to. Keeping a record of what you have shared will ensure your establishment can meet this requirement.

Only keep collected information for 30 days

Routinely and securely destroy information collected after 30 days. A suggested practice would be to delete 31-day old information at the same time you add daily contact information. Any papers containing personal information should be securely shredded rather than just placing them in a garbage can or recycling bin.

Properly secure the collected information

Your organization must make reasonable security arrangements to protect personal information in its custody or under its control. For example, if the collected information is in paper form, it should not be left in a publicly accessible area. Rather, it should be stored in a locked file cabinet. If you are storing the list on a computer, make sure the computer is password protected, encrypted, and on a secure network. Position computer monitors so that personal information displayed on them cannot be seen by visitors.

Conclusion

If you have any questions about how to collect, use, disclose or protect personal information at your establishment, call us at (250) 387-5629 or email us at info@oipc.bc.ca. Other toll-free numbers are available [here](#).

If collected personal information is stolen or lost (also known as a privacy breach), contact our office for assistance.

These guidelines are for information purposes only and do not constitute a decision or finding by the Office of the Information and Privacy Commissioner for British Columbia. These guidelines do not affect the powers, duties, or functions of the Information and Privacy Commissioner regarding any complaint, investigation, or other matter under FIPPA or PIPA.