Best Practices for Protecting Individual Privacy in Conducting Survey Research

Information and Privacy Commissioner of Ontario

Commissaire à l'information et à la protection de la vie privée de l'Ontario

CONTENTS

FOREWORD

This paper was first published in 1999 as a result of the Ontario Public Service Restructuring Secretariat asking ministries to assess their services to the public and to subsequently develop action plans to improve any detected service gaps. Given the anticipated volume of survey research and that such research may involve the collection, retention, use, disclosure, and disposal of personal information, the Office of the Information and Privacy Commissioner (IPC) collaborated with the Ministry of Labour and the Corporate Freedom of Information and Privacy Office of Management Board Secretariat (now the Ministry of Government and Consumer Services) to develop best practices for protecting individual privacy in conducting survey research.

Since the original publication of this paper, significant changes have taken place in information and communications technologies which have affected the way in which survey research is conducted. For example, it is now common for survey research to be conducted online and for individuals to use a cellphone instead of a landline. Government institutions have requested further guidance as a result of these changes. Accordingly, we have updated this paper to reflect these changes and to address the privacy issues raised by the use of new information and communications technologies in the conduct of survey research.

The first version of *Best Practices for Protecting Individual Privacy in Conducting Survey Research* was accompanied by a condensed version and a summary of the best practices. The current version consolidates these three pieces into a single publication.

The IPC gratefully acknowledges the work of staff at the Ministry of Labour and the Corporate Freedom of Information and Privacy Office, Management Board Secretariat, whose contributions made it possible to develop the original version of this paper and the best practices.

INTRODUCTION

As government institutions strive to become more efficient, accountable and customer focussed, they frequently seek input from the public about their programs and services. One of the most cost-effective ways to elicit this input is through survey research.

Survey research can be used to help plan new programs and services, or modify existing programs or services or the manner in which they are delivered, and to help ensure that the programs and services that are provided meet the needs and expectations of customers. Survey research can be used to obtain input from a wide range of individuals, including the direct or potential recipients of programs and services, the staff and managers responsible for planning and delivering programs and services, and the public at large.

While survey research can be an important tool for shaping government programs and services, it may involve the collection, retention, use, disclosure, and disposal of personal information. *Personal information* is defined in section 2(1) of the *Freedom of Information and Protection of Privacy Act* (the provincial *Act*) and the *Municipal Freedom of Information and Protection of Privacy Act* (the municipal *Act,* together with the provincial *Act:* the *Acts*) as "recorded information about an identifiable individual." However, for the purposes of sections 38 and 39 of the provincial *Act* and sections 28 and 29 of the municipal *Act*, which deal with the collection of personal information, the definition of "personal information" is modified to include information about an identifiable individual that is not recorded.[1] Because of this, the *Acts* place restrictions on the collection of personal information in either recorded or unrecorded form. Examples of personal information include an individual's name, address, telephone number, age, sex, and his or her personal opinions or views.

Whenever provincial and municipal institutions collect, retain, use, disclose, or dispose of personal information, they are required to comply with the privacy protection provisions of the *Acts*, and their regulations. To help institutions comply with the *Acts*, this paper details the privacy considerations at each stage in the design and implementation of survey research projects and recommends some best practices which are based on the provisions of the *Acts* and their regulations. For ease of reference, these best practices are compiled into a "checklist" tool at the end of the document (see Appendix A). Institutions may wish to use this tool as an aid in reviewing the relevant privacy issues at each stage of their survey research project.

Depending on factors such as whether the survey research involves "personal health information" and whether the person conducting the research is a "health

1 See section 38(1) of the provincial *Act* and section 28(1) of the municipal *Act*.

information custodian" or received the personal health information from a health information custodian, the survey research may fall under the provisions of the *Personal Health Information Protection Act* (*PHIPA*). While the practices developed in this paper may provide some guidance for conducting survey research in any context, they do not address any specific concerns related to research conducted under *PHIPA*.

It is important to note that under section 65(8.1) of the provincial *Act*, certain research records of an educational institution or a hospital are excluded from the application of the *Act*. Notably, records respecting or associated with research conducted or proposed by an employee of an educational institution or person associated with an educational institution and records respecting or associated with research, including clinical trials, conducted or proposed by an employee of a hospital or person associated with a hospital are not subject to the provincial *Act*.[2] Nevertheless, the best practices described in this document, particularly those relating to limiting the collection of personal information, may still provide guidance even though the legal provisions mentioned in the practices may not be strictly applicable.

In general, survey research raises two central privacy considerations. The first is the potential collection of personal information from survey research participants. The second is the potential use of previously collected personal information for the purpose of obtaining a sample of survey research participants. With respect to the first consideration, the position advocated in this paper is that for most survey research, personally identifiable survey data is only required in very limited and specific circumstances. To the extent that the collection of personal information can be avoided, the privacy considerations will be minimized. However, with respect to the second consideration, it is often not possible to avoid the use of personal information altogether. Even where survey research is conducted anonymously (i.e., results in "de-identified" survey responses), personal information may still be needed to obtain a sample of survey research participants. Therefore, individual privacy and compliance with the *Acts* will be a consideration in most cases.

In addition, the use of online surveys or online survey providers may involve the collection of personal information as a result of "metadata" being automatically passed or gathered from a survey participant's device or computer. For example, when using an online survey provider, the Internet Protocol (IP) address used by a survey participant's device or computer will be automatically passed to the provider. To the extent that metadata involves personal information (in that it identifies, or may be used in combination with other information to identify, a

2 Note that sections 65(9) and 65(10) of the provincial *Act* set out exceptions to section 65(8.1) that may apply to the survey.

survey participant), the collection, retention, use and disclosure of metadata will also engage the *Acts*.[3]

For the purposes of this paper, the process of conducting survey research projects has been divided into eight stages:

- issue definition;
- research design and questionnaire development;
- pre-testing;
- sample selection;
- data collection;
- data analysis;
- reporting of results; and
- data archiving.

Where the *Acts* are cited, the sections of the provincial *Act* appear first, followed by a slash (/) and the corresponding sections of the municipal *Act*, e.g., 38(2)/28(2).

For those individuals who are not familiar with the relevant provisions of the *Acts* cited in this paper, your institution's Freedom of Information and Privacy Coordinator or the Ministry of Government and Consumer Services may be able to assist you in complying with the requirements of the legislation in developing and conducting surveys. The IPC is also available to review and comment on any privacy issues that may arise as you develop and implement your research plan.

3 See Office of the Privacy Commissioner of Canada, "Metadata and Privacy: A Technical and Legal Overview," October 2014, https://www.priv.gc.ca/information/research-recherche/2014/md_201410_e.asp.

PRIVACY CONSIDERATIONS AT EACH STAGE OF A SURVEY RESEARCH PROJECT

STAGE 1: ISSUE DEFINITION

Before developing a survey, it is important to clearly define the issues you wish to address through the survey. In doing so, you must assess the purposes and focus of the survey. For example, is the purpose to gather information to help plan new programs or services, to identify gaps in existing program/service delivery, etc.?

Clearly defining the purposes of the survey will help limit the collection of information to that which is strictly necessary. In survey research that requires the collection of personal information, a clear understanding of the purposes of the survey will help to minimize the collection of personal information.

Under sections 39(2)(b)/29(2)(b) of the *Acts*, whenever personal information is collected, an institution is required to inform the individual to whom the information relates of the principle purpose or purposes for which the personal information will be used. In general, once the individual has been informed of the purposes for the collection, the collection, use and disclosure of that information should be limited to that which is necessary to fulfil the specified purposes.[4] Thus, clearly defining the purposes of the survey is a precondition for determining what information needs to be collected, and how that information may be subsequently used and disclosed.

STAGE 2: RESEARCH DESIGN AND QUESTIONNAIRE DEVELOPMENT

During the early stages of designing a survey, a number of key issues which may have implications for privacy protection need to be resolved. These issues include deciding who will conduct the survey, whether it will be necessary to collect personal information, whether you have the legal authority to collect the personal information, and the most appropriate type of survey research method to use.

4 There are circumstances in which personal information collected for one purpose may be used or disclosed for another purpose, e.g., if the other purpose is consistent with the original purpose or if the individual to whom the information relates identifies the information and consents to the use or disclosure. See sections 41(1)/31 and 42(1)/32 of the *Acts*. See also sections 43/33 for a definition of "consistent purpose."

WHO WILL CONDUCT THE SURVEY?

At some point during the survey research project, you need to decide whether the survey will be conducted by internal staff, by staff of another provincial or municipal institution, or by a third party, such as an external consultant or an online survey provider. Regardless of who conducts the research, full accountability for the privacy and security of personal information always remains with the institution.

Whenever staff of an institution conduct survey research, terms of reference should set out the requirements for the secure collection, retention, use, disclosure and disposal of personal information, in accordance with the *Acts*. (A sample terms of reference is contained in Appendix B.) Whenever external consultants or private companies conduct survey research on behalf of an institution, they are subject to the same general limitations on collection as the institution itself. The institution is also ultimately responsible for the use, disclosure and disposal of personal information in its custody and/or control, even if external consultants or private companies conduct the research. In such cases, contractual agreements should be established to clarify the obligations of external consultants or private companies to securely collect, retain, use, disclose and dispose of personal information, in accordance with the *Acts*. Contractual agreements should also ensure institutions retain control over any personal information that may be involved in survey research. For information on how to evaluate and develop appropriate contractual agreements, see the Office of the Chief Information and Privacy Officer's "Guidelines for the Protection of Information when Contracting for Services" (available by contacting the Information, Privacy and Archives Division, Ministry of Government and Consumer Services[5]).

It is important that you review either the terms of reference or the contractual agreement periodically during the survey and at the completion of it, to ensure that all conditions set out in either document have been fully complied with.

ONLINE SURVEY PROVIDERS

The rise of the Web as a communications platform has led to the establishment of a new kind of service for conducting survey research. Online survey providers offer web-based services and tools for conducting survey research online. They afford researchers many conveniences and efficiencies, especially in comparison to their offline alternatives. For example, many online survey providers offer standard templates or "wizards" to assist users in creating surveys; are able to instantly compute and display survey results; and provide storage and backups of survey data. In addition, many online survey providers offer tiered versions of

5 The Information, Privacy and Archives Division may be contacted by email at web.foi.MGCS@ontario.ca or by telephone at 416-212-7061.

their services, with different functionality available at different costs. Oftentimes this includes a "basic" version free of charge.

While convenient and efficient, and oftentimes cost effective, the use of online survey providers raises some privacy concerns that must be addressed in order to ensure compliance with the *Acts*. In general, there are three issues to consider.

1. Online Survey Providers May Allow Third Parties to Track Survey Participants

The majority of websites today are a mix of "first-party" content provided by the website operator and "third-party" content or services (embedded within the first-party content) provided by other websites or online entities. Examples of third-party content or services include advertisements, social media widgets and website analytics.

This mix of first-party and third-party content has given providers of third-party content or services the ability to track websites visited by individuals across the Web. These providers are able to do this through various techniques; however, the standard method involves a web technology called "cookies."[6]

When you use an online survey provider, survey participants will be directed to the provider's website. If the online survey provider's website has third-party content or services embedded within it, the provider(s) of that third-party content may be able to track which survey participants visited the online survey provider's website. The provider(s) of third-party content or services may then use this information to create or further develop user profiles of survey participants. Such profiles are used to target individuals with online content (mostly advertisements). They typically combine information from other available sources in order to increase the level of detail and insight into the individual. Because of this, these profiles will generally be considered to be personal information.[7]

As a general rule, the online tracking of survey participants by providers of third-party content or services will not be in compliance with the *Acts* because this collection will have been done on behalf of the institution but without legal justification in the *Acts*. This holds true even in the case where the survey data itself does not involve personal information.

Accordingly, where staff of your institution use an online survey provider to conduct the survey, you should not use an online survey provider that allows third parties to track survey participants.

---

6 Other techniques that may be used by providers of third-party content or services to track websites visited by individuals include "supercookies" and device or browser "fingerprinting."

7 See Office of the Privacy Commissioner of Canada, "Policy Position on Online Behavioural Advertising," 2012, https://www.priv.gc.ca/information/guide/2012/bg_ba_1206_e.asp.

2. Online Survey Providers Control the Terms of Service, Not You

When considering using an online survey provider, it is important to recognize that most providers offer their services on a take-it-or-leave-it basis through standardized terms-of-service agreements and privacy policies found on their websites. In comparison to the case of an external consultant where you take part in establishing the provisions of the contractual agreement, this marks a significant shift in control over the policies governing the privacy and security of the survey research.

Nevertheless, the fact that you did not take part in establishing the requirements of the service agreement does not absolve you of your responsibility to ensure that the processing of any personal information done by the online survey provider on your behalf complies with the *Acts*. Therefore, whenever staff of your institution use an online survey provider to conduct survey research that involves personal information, it is your responsibility to ensure that the provider's terms-of-service agreement and privacy policy allow for the secure collection, retention, use, disclosure, security and disposal of personal information in accordance with the *Acts*. The provider's terms-of-service agreement and privacy policy should contain generally equivalent provisions to those established for external consultants' obligations.

In addition, because an online survey provider controls the terms-of-service agreement and privacy policy, it may decide to update these documents and alter the terms and conditions set out in them. The level of risk this poses to privacy changes based on whether or not your survey research involves personal information. If your survey research involves personal information, the level of risk is high. Accordingly, you should ensure that the terms of service between the online survey provider and the institution are not subject to change without the express written consent of the institution. On the other hand, if your survey research does not involve personal information, express consent for any changes in the terms of service is not required. Instead, you should review the provider's terms-of-service agreement and privacy policy periodically during the survey, at the completion of it, and while the survey information is stored by the provider, to ensure that the terms and conditions set out in those documents have not changed or continue to comply with the *Acts*.

3. The Survey Data May Be Stored Outside of Canada

Another issue to consider in deciding whether to use an online survey provider is where the survey data will be stored. Although accessed from within Ontario, an online survey provider may store information it collects outside of the province or Canada depending on the location of its servers. Survey data stored outside of Ontario or Canada may be subject to the laws of the jurisdiction in which it

resides, and the level of protection provided by those laws may differ from the level of protection required by the *Acts*.

In Ontario, there is no legislative prohibition against the storing of personal information outside of the province or Canada. However, the *Acts* and their regulations require government institutions to ensure that reasonable measures are in place to protect the privacy and security of the personal information in their custody or control.

If an online survey provider's servers are based outside of Ontario or Canada, you should evaluate the risk this extraterritorial storage of information poses to the privacy and security of the survey data in consultation with your access and privacy professionals. In so doing, you should take into consideration the sensitivity of the information, the laws of the jurisdiction in which the personal information is stored, and the extent to which safeguards, including contractual provisions, can be used to mitigate the risk, if any. If the risk is high and the effectiveness of the safeguards is uncertain, then you should consider using a different online survey provider or conducting the survey research in another manner. For additional guidance on U.S.-based service providers, please see the IPC's Privacy Investigation Report PC12-39 *Reviewing the Licensing Automation System of the Ministry of Natural Resources*.[8]

SELF-HOSTING

If you want to conduct survey research online but do not wish to use an online survey provider, there are a number of software programs or apps, some of which are "open source" and/or freely available, that support the option of self-hosting where the program that runs the online survey can be installed and hosted on your own organization's web servers. The advantage of this approach is that it avoids the use of online survey providers. As such, it can mitigate concerns about whether a provider's terms-of-service agreement and privacy policy comply with the Acts. It can also mitigate data residency concerns by affording you more control over where the survey data is stored and who has access to it. The disadvantage, however, is that you must have the necessary technical resources to securely install, operate and maintain the survey software and data.

MINIMIZING THE COLLECTION OF PERSONAL INFORMATION

During the early stages of research design, determine what information needs to be collected from survey research participants and whether any of the information qualifies as personal information. This is an important issue to consider up-front, because institutions are not required to comply with the

8 Available at: https://www.ipc.on.ca/images/Findings/2012-06-28-MNR_report.pdf.

privacy protection provisions of the *Acts* with respect to information that falls outside the definition of personal information (see parts III/II of the *Acts*). If there is any ambiguity about whether the information to be collected is personal information, you should err on the side of caution by complying with the *Acts.*

Determining whether you need to collect personal information, as defined under the *Acts*, may not be straightforward. In making this determination, consider who will be included in the target population, the nature of the information that will be requested from participants, and the extent to which the survey responses will identify or could be used, either alone or with other information, to identify an individual.

It may be helpful to conduct a privacy impact assessment (PIA), which can help identify potential privacy concerns in designing and conducting the survey as well as possible ways to mitigate them. Organizations may wish to refer to the Ministry of Government and Consumer Services' guidance on conducting a PIA (available by contacting the Information, Privacy and Archives Division of the Ministry[9]) or the IPC's *Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act* (which provides guidance on conducting a PIA in the context of *PHIPA* rather than the *Acts*).[10]

The views and opinions elicited by the survey may not clearly fall within the definition of personal information. For example, if the survey has been designed to elicit the views and opinions of employees or others in their professional capacity, the information may not fall under the definition of personal information.[11]

Also, regardless of whether information is defined as personal information for the purposes of the *Acts*, survey participants may have concerns about the manner in which their views and opinions expressed through the survey research are used and disclosed. Moreover, institutions are required to not collect more personal information than is necessary. Therefore, whenever possible, conduct surveys anonymously, ensuring that the survey responses are de-identified (i.e., do not identify and cannot be used, either alone or with other information, to identify survey participants). Conducting surveys anonymously is the best way of ensuring the privacy of survey participants.

ANONYMOUS SURVEYS

In designing any survey, always consider the possibility of collecting information such that the survey data do not identify and cannot be used, either alone or with other information, to identify survey participants. To the extent that the survey can be conducted anonymously, the risk of unauthorized collection, use

9 See n. 5 above.

10 Available at: https://www.ipc.on.ca/images/Resources/up-phipa_pia_e.pdf.

11 See IPC Orders P-1524 and MO-2790.

and disclosure of personal information will be kept to a minimum. Moreover, in conducting anonymous surveys, compliance with the *Acts* is not required.

It is important to recognize that certain survey research methods are less amenable to conducting anonymous surveys than others. For example, email surveys require participants to send their responses back to the survey conductor via email. However, unlike physical mail where messages can be sent anonymously, i.e., without a return address, email messages always contain the email address of the sender. Because of this, email surveys make it difficult, if not impossible, to conduct anonymous surveys.

The first step in conducting an anonymous survey is to retrieve survey responses in such a way as to remove any link between the personal information used to contact survey participants and their survey responses. In mail surveys, this may be achieved by having participants mail back their anonymous questionnaire in a pre-printed, postage-paid envelope with no return address. In online surveys, this same kind of separation may be done programmatically in the software.

Although necessary, separating individuals' contact information from their survey responses is not sufficient to render the survey anonymous and de-identify the responses. Additional work must be done to ensure that the survey responses themselves do not contain what are known as "quasi-" or "indirect identifiers." These are variables that may be used to single out individuals without directly identifying them. A classic example is the combination of gender, date of birth and postal code. While these variables do not in and of themselves identify anyone, when taken together they will in most cases be unique to a single individual. Because of this, they may be used to form links to other information or datasets, which may in turn identify the individual.

While anonymous surveys may be ideal from a privacy perspective, they present a number of research design challenges. One challenge is that, since there is no direct way of knowing who has responded to an anonymous survey, it will be difficult to follow up with those individuals who do not respond. A lack of follow-up could result in a poor response rate and, consequently, the validity of the results of the survey could be questioned. However, to help ensure an adequate response rate, follow-up could be accomplished by contacting all potential participants regardless of whether they responded.

Alternatively, participants could be provided with another means of indicating that they had responded (e.g., they could mail in a postcard containing their name or some other personal identifier indicating that they had responded, at the same time as they mail in their anonymous questionnaire). Then, follow-up could be carried out with only those participants who have not yet confirmed that they have responded.

In the case of online surveys, survey participants may be provided with an invite code or customized link to the survey that allows the system to determine whether a particular individual has responded or not. However, this information should not be associated with or linked to the survey data or else the survey may not be considered anonymous.

Another challenge is that anonymous surveys do not permit verification or clarification of information provided by survey participants. In addition, anonymous survey data cannot be linked to information obtained in successive surveys or to information available through other sources such as a client or customer database. While this will not be an issue in most survey research, in some circumstances there may be a clear rationale for linking information across time and/or sources or for following up with participants.

METADATA AND ANONYMOUS SURVEYS

Where an anonymous survey is conducted online, either through an online survey provider or other means, additional measures are required to protect the privacy of the survey participants. For example, when a survey participant's device or computer connects to an online survey, additional information about the connection is automatically passed to the hosting system. This "metadata" includes the Internet Protocol (IP) address used by the survey participant's device or computer, the uniform resource locater (URL) of the resource that referred the participant to the survey and any invite codes generated by the survey system. Similar to quasi- or indirect identifiers, metadata may be used in combination with other information to identify a survey participant.

When conducting an anonymous survey online, you should ensure that the hosting system does not link or associate with the survey data any information automatically passed to it from a survey participant's device or computer that may be used to identify the individual.

In certain cases, linking or associating metadata with the survey data may be required to ensure the integrity of the survey results. For example, if the survey is conducted online and does not have a fixed sample of participants but is rather available to anyone who visits an institution's public-facing website, then it may be necessary to collect and associate with the survey data some forms of metadata (e.g., IP address) in order to ensure that the results were not skewed by individuals retaking the survey multiple times. While this approach may help to ensure the integrity of survey results,[12] because it links or associates information that may identify individuals, either alone or in combination with

12 It is important to note that a single IP address may be shared by many Internet users at the same time. Therefore, a challenge to this approach is that the rejection of survey results from the same IP address may in fact affect valid submissions.

other information, with the survey data, it also precludes the survey from being considered anonymous.

On the other hand, the integrity of survey results may be improved, if not assured, through privacy-protective alternatives that do not link or associate identifiable information with the survey data. For example, once a survey is submitted from a particular IP address, a moratorium on additional submissions from the same IP address could be established for a given period of time, e.g., 24 hours. This would limit multiple submissions, while still allowing individuals who share an IP address to take the survey. In addition, the use of a CAPTCHA ("Completely Automated Public Turing test to tell Computers and Humans Apart") could be used to ensure that survey submissions are not being automated.

When conducting an online survey that does not have a fixed sample of participants (i.e., where the survey may be taken by anyone), you should consider privacy-protective alternatives for improving the integrity of the survey results.

CODED SURVEYS

An alternative to having completely anonymous survey responses would be to replace all personally identifiable data in the survey with a special code. This special code should not, in and of itself, identify the individual but should be used to link the survey data with personal information for limited and specific purposes (e.g., to facilitate follow-up and the linking of information across time and sources).

The survey data with the special code should be retained separately from the personal information that identifies participants. The only link between the two sets of data should be the special code. Access to the personal information through the special code should be limited to those individuals with a need-to-know for specific, defined purposes, as outlined above.

If the survey is to be coded in this manner, potential participants should be informed of this procedure and its purpose prior to participation in the survey. Also, survey data with this type of coding falls within the definition of personal information. Therefore, you are required to comply with the *Acts* with respect to the secure collection, retention, use, disclosure and disposal of this personal information.

PERSONAL INFORMATION NOT DIRECTLY RELATED TO THE SURVEY

In some cases, you may want to collect personal information at the same time that you collect responses to the survey for a purpose not directly related to the current survey. For example, you may want survey participants to provide

personal information, such as name, address and/or telephone number, so that you may provide them with information about the programs or services offered by your institution, provide them with a summary of the survey results or contact them as potential participants in subsequent research projects.

In such cases, since there is really no need to link the personal information to the survey responses, survey participants should **not** be asked to provide this information with their responses. The two types of information should be collected separately and, if possible, sent to different addresses or personnel. For example, in printed mail surveys, participants could be provided with a separate postcard containing their personal information (i.e., name, address and/or telephone number) to mail to your institution indicating their desire to receive further information and/or their agreement to be contacted for subsequent research projects. In online surveys, participants could indicate their preference after completing the survey and the separation of survey data and personal information could be achieved programmatically in the software.

IF YOU NEED TO COLLECT PERSONAL INFORMATION, DO YOU HAVE THE AUTHORITY?

If you determine that it will be necessary to collect personal information in the course of conducting a survey, assess whether you have the legal authority to collect the personal information under sections 38(2)/28(2) of the *Act*s.

Sections 38(2)/28(2) of the *Acts* set out the conditions under which personal information may be collected. Specifically, they state: "No person shall collect personal information on behalf of an institution unless the collection is expressly authorized by statute, used for the purposes of law enforcement or necessary to the proper administration of a lawfully authorized activity."

If **none** of these three conditions exists, you do **not** have the authority to collect the personal information under the *Acts*. Where you determine that you do not have the authority to collect personal information, you may only conduct an anonymous survey, as discussed previously.

DETERMINE THE MOST APPROPRIATE SURVEY RESEARCH METHOD

In designing your survey, select a survey research method that will elicit the desired information from survey respondents (e.g., mail, telephone, personal interviews, focus groups, e-mail, online survey). However, some methods are more intrusive than others. For example, receiving a questionnaire in the mail may be less intrusive than a telephone survey.

The nature of the information to be requested in the survey should be considered when determining the most appropriate method to use. For

example, you would probably not choose a telephone survey to elicit sensitive information about an individual, but rather a less intrusive method, such as an anonymous questionnaire.

STAGE 3: PRE-TESTING (FINE-TUNING) THE SURVEY

When you pre-test the survey, you may collect personal information about pre-test participants. Therefore, apply the best practices discussed in this paper to any personal information collected during the pre-test phase of the project.

STAGE 4: SAMPLE SELECTION

Even if a survey is conducted anonymously, you may still need to collect or use personal information to obtain a survey research sample. The sample can be obtained in a number of ways depending on the purposes for conducting the survey. Some of the more common methods of obtaining a survey research sample are as follows:

- by contacting those individuals with whom your institution has had direct contact in the context of the programs or services that it provides (i.e., using the personal information previously collected from your direct customers or clients);
- by contacting those individuals on a list obtained from another institution or third party (i.e., indirectly collecting personal information that was previously collected by another institution or third party); and
- by asking another institution or third party to contact individuals on your behalf (i.e., by having another institution or third party use personal information previously collected from its customers or clients).

Depending on which method is used to obtain your survey research sample, different privacy issues need to be addressed. The privacy considerations associated with each method are discussed below.

USING PERSONAL INFORMATION PREVIOUSLY COLLECTED FROM YOUR CUSTOMERS OR CLIENTS

In conducting surveys of your direct customers or clients, you may need to use personal information that has already been collected from them to obtain the survey research sample. Usually, personal information, such as name and address, telephone number, or email, is only needed to contact potential survey participants. However, in some cases, additional personal information (e.g., age, gender, education, and income) may be needed to select a sample with specific

characteristics. In most cases, this client or customer information would have been collected within the context of delivering the programs or services that are the focus of the survey.

PROVIDING NOTICE AT THE TIME OF COLLECTION

If you anticipate that customer or client information will be used to obtain a survey research sample, then the appropriate notice of this use should be provided at the time of collection. The subsequent use of the personal information for this purpose would be in compliance with sections 41(1)(b)/31(b) of the *Acts*, since you would be using the personal information for the purpose intended at the time of collection.

Sections 39(2)/29(2) of the *Acts* state that where personal information is collected on behalf of an institution, the head shall, unless notice is waived by the responsible minister, inform the individual to whom the information relates of:

(a) the legal authority for the collection;

(b) the principal purpose or purposes for which the personal information is intended to be used; and

(c) the title, business address and business telephone number of a public official who can answer the individual's questions about the collection.

NO NOTICE PROVIDED AT THE TIME OF COLLECTION

Although providing notice of the use of personal information for survey research purposes is always the best practice, in some circumstances the *Acts* may permit the use of personal information for this purpose even though no notice was provided at the time of collection.

Sections 41(1)/31 of the *Acts* address the *use* of personal information. These sections state, in part,[13] that an institution shall not use personal information except:

(a) where the person to whom the information relates has identified that information in particular and consented to its use;

(b) for the purpose for which it was obtained or compiled or for a consistent purpose; or

(c) for a purpose for which the information may be disclosed to the institution under sections 42/32 of the *Acts.*

13 Note that the provincial *Act* provides that an educational institution may use personal information in its alumni records and a hospital may use personal information in its records for the purpose of its own fundraising activities, if the personal information is reasonably necessary for the fundraising activities, subject to additional requirements. See sections 41(1)(d), 41(2) and 41(3) of the provincial *Act.*

Under paragraph (a), personal information could be used to select a survey research sample if the individual has consented to this use. However, in many cases it will not be reasonable or practical to obtain consent from every potential survey participant and you will have to assess whether you may use the personal information for this purpose under paragraph (b).

In most customer or client surveys, the personal information that would be used to obtain a survey research sample would have been obtained within the context of providing the service or program which is the focus of the survey. The *Acts* state that where personal information has been collected *directly* from the individual to whom it relates, the purpose of a use of that information is a consistent purpose (sections 41(1)(b)/31(b) of the *Acts*) only if the individual *might reasonably have expected* such a use (sections 43/33 of the *Acts*). Where personal information has been collected *indirectly* from another source, the purpose of a use of that information is a consistent purpose only if it is *reasonably compatible* with the purpose for which it was obtained or compiled.[14]

Sections 41(1)(c)/31(c) do not apply when you obtain the survey sample through the use of information previously collected from your direct clients or customers. They may apply when the survey sample is obtained through the collection of information from another institution, as discussed below.

COLLECTING PERSONAL INFORMATION FROM ANOTHER INSTITUTION OR THIRD PARTY

In conducting surveys of individuals other than your direct customers or clients, you may wish to select your survey sample through the collection of personal information from another institution or third party. This is considered to be an *indirect collection* of personal information under the *Acts*.

Sections 39(1)/29(1) of the *Acts* require that personal information be collected directly from the individual to whom it relates, unless certain circumstances listed in sections 39(1)/29(1) exist (e.g., where the individual authorizes another manner of collection, where another manner of collection is authorized by or under a statute, etc.). If you intend to collect personal information indirectly, you must determine whether you have the authority to do so under sections 39(1)/29(1).

Sections 39(1)(c)/29(1)(c) of the *Acts* permit the indirect collection of personal information where the IPC has authorized this manner of collection under sections 59(c)/46(c). Sections 59(c)/46(c) state that the IPC may, in appropriate circumstances, authorize the collection of personal information other than directly from the individual. Where no other provisions in sections 39(1)/29(1)

14 See IPC Privacy Complaint MC-060007-1.

authorize this manner of collection, you should apply to the IPC for authorization by completing an Application for Indirect Collection, available from the IPC.[15]

COLLECTING INFORMATION FROM PUBLIC RECORDS FOR SAMPLE SELECTION

Public databases are one source of information that may be used to compile lists of potential research participants. A list of public databases can be found in the Ministry of Government and Consumer Services' annual Directory of Records.[16] The list includes public databases such as the Personal Property Security Registration System and the Land Registration System.

Under sections 37/27 of the *Acts*, public databases are excluded from the privacy protection provisions of the *Acts.* The rationale for this exclusion is that there are legitimate needs for this information to be widely available to the general public, and imposing restrictions on the use and disclosure of this information under the *Acts* would not be appropriate. Although public databases are excluded from the privacy provisions of the *Acts*, this does not mean that there are no privacy implications in the collection, use and disclosure of this information for unintended purposes without the knowledge and consent of individuals.

The privacy investigation reports of the IPC have generally found that under sections 37/27, personal information that is maintained by an institution may be excluded from the application of the *Acts* only if the personal information is maintained by that institution specifically for the purpose of creating a record which is available to the general public. Other institutions cannot claim the exclusion unless they also maintain the personal information for this purpose. Consequently, you may only collect personal information contained in a public database if you have the authority to collect the personal information under sections 38(2)/28(2) of the *Acts*.[17]

COLLECTING INFORMATION FROM ANOTHER INSTITUTION'S PERSONAL INFORMATION BANKS FOR SAMPLE SELECTION

Another possible source of information that may be used to compile lists of potential research participants is the personal information maintained by other government institutions or other third parties. When institutions obtain a survey research sample in this manner, this is referred to as *data sharing.*

15 For information about the indirect collection of personal information, see *Practices No. 14 – The Indirect Collection of Personal Information*, available at: https://www.ipc.on.ca/images/Resources/up-num_14.pdf; For an application, see "Indirect Collection Guidelines – Appendix A," available at: https://www.ipc.on.ca/english/Resources/Best-Practices-and-Professional-Guidelines/Best-Practices-and-Professional-Guidelines-Summary/?id=394, and "Indirect Collection Guidelines – Appendix B," available at: https://www.ipc.on.ca/english/Resources/Best-Practices-and-Professional-Guidelines/Best-Practices-and-Professional-Guidelines-Summary/?id=395.

16 Available at: https://www.ontario.ca/government/directory-records.

17 See IPC Investigations I96-018P and PC-980049-1.

The sharing of personal information between two organizations runs counter to two of the most fundamental principles of data protection — that personal information should be collected directly from the individual to whom it pertains and should only be used for the purpose for which it was collected (with limited exceptions). Data sharing respects neither of these principles since the personal information is collected indirectly and used for a purpose for which it may not have been intended at the time of collection.

Data sharing between organizations may lead to individuals' loss of control over their personal information. Therefore, information sharing should not occur without exploring less privacy-intrusive means of meeting the objectives of the survey. Before making a decision to share personal data, consider all practical alternatives which are more privacy protective. You should also consider the merits of any contemplated data sharing and whether sharing is appropriate.

Any sharing of personal information should be supported by a written *data sharing agreement*. Such an agreement will clarify the rights and obligations of all parties to ensure compliance with the *Acts*. To prepare such an agreement, refer to the IPC's *Model Data Sharing Agreement*.[18] Among other things, the agreement should specify the authority of the institution to collect the personal information in question under sections 38(2)/28(2) of the *Acts*. In addition, if the party maintaining the personal information bank is an institution subject to one of the *Acts*, the agreement should specify its authority to use and disclose the personal information for this purpose under sections 41/31 and 42/32 of the *Acts,* respectively.

One of the exceptions that an institution maintaining the personal information bank may rely on to disclose this personal information is found in sections 42(1)(a)/32(a) of the *Acts*, which state that an institution shall not disclose personal information in its custody or under its control except in accordance with Parts II/I. Sections 21(1)(e)/14(1)(e) fall under Parts II/I and state that an institution may disclose personal information that identifies an individual to a person other than the individual to whom the information relates for a **research purpose**, when certain conditions are met. These conditions are:

- the disclosure must be consistent with the conditions or reasonable expectations of disclosure under which the personal information was provided, collected or obtained;
- the research purpose for which the disclosure is to be made cannot be reasonably achieved unless the information is provided in a form which allows individuals to be identified; and

18 Available at: https://www.ipc.on.ca/images/Resources/model-data-ag.pdf.

- the person who is to receive the record must agree to comply with all of the conditions relating to security and confidentiality prescribed by section 10(1) of Regulation 460/section 10(1) of Regulation 823.

One of the conditions set out in the regulations is that the recipient of the information must obtain written authority from the institution maintaining the personal information in order to contact, either directly or indirectly, any individual to whom the personal information relates.

Section 10(2) of Regulation 460 and section 10(2) of Regulation 823 made under the *Acts* require that an agreement relating to the security and confidentiality of personal information to be disclosed for a research purpose be in *Form 1*, which is set out in the regulations.

OBTAINING YOUR SURVEY RESEARCH SAMPLE INDIRECTLY FROM ANOTHER INSTITUTION OR THIRD PARTY

In some cases, it may be possible to avoid collecting personal information to obtain a survey research sample. This could be done by asking another institution or third party to use the information that it maintains (e.g., information in a public database or personal information bank) to contact potential research participants directly on your behalf. For example, an institution or third party could be asked to mail the surveys directly to potential participants. If the survey is an anonymous survey, participants could be asked to return their anonymous surveys directly to the institution conducting the research. The institution conducting the survey would thereby avoid the collection of personal information altogether.

However, if the survey is not anonymous, the institution conducting the survey research must have the authority to collect the personal information under sections 38(2)/28(2) of the *Acts*. In addition, all potential participants should be provided with the proper notice of collection of personal information by the institution conducting the survey, as required under sections 39(2)/29(2) of the *Acts*.

Regardless of whether the survey is conducted anonymously, the institution maintaining the information (as distinguished from the institution conducting the survey) must assess whether it has the authority, under sections 41/31 of the *Acts*, to use the information to contact potential research participants on behalf of the institution conducting the research.

IMPLICATIONS FOR PERSONAL INFORMATION BANKS

Regardless of whether notice was provided at the time of collection, if you use personal information to obtain a survey research sample, ensure that you comply

with the requirements for personal information banks set out under sections 44 to 46 of the provincial *Act,* and sections 34 and 35 of the municipal *Act*. "Personal information bank" means a collection of personal information that is organized and capable of being retrieved using an individual's name or an identifying number or particular assigned to the individual.

If personal information is to be used for survey research purposes on a regular basis, then this should be specified in the index of personal information banks, as required under sections 45(d)/34(1)(d) of the *Acts*. Where survey research has not been included in the index of personal information banks as a regular use of the information, sections 46(1)(a)/35(1)(a) of the *Act*s require that you attach or link to the personal information a record of this use. In addition, if the use has not been included in the index, section 46(3) of the provincial *Ac*t requires that the responsible minister be notified and the use be included in the index in the future. Under section 34(2) of the municipal *Act,* you must ensure that the index is amended as required to ensure its accuracy.

STAGE 5: DATA COLLECTION

CONTACTING POTENTIAL PARTICIPANTS IN THE SURVEY

The fact that an individual has received one of your institution's programs or services could be considered to be sensitive personal information. When contacting potential survey participants, ensure that you do not invade their privacy by inadvertently disclosing this information to third parties, such as family members or co-workers.

For example, when contacting potential participants by mail, your institution name should not be printed on the outside of the envelope, as this information could reveal to others residing in the household that the individual has some relationship with your institution. Similarly, when contacting potential participants by telephone, do not disclose the personal information of the potential participant by identifying your institution or the purpose of the telephone call in a voice mail message or a message taken by a third party who happens to answer the telephone. Take reasonable steps to verify the potential participant's identity before providing further information. Also, steps should be taken to ensure that the name of your institution is not inadvertently disclosed to third parties through telecommunications technology such as caller identification.

For telephone surveys, the widespread use of cellphones should be taken into consideration. Due to their mobility, cellphones increase the chances that potential participants of a telephone survey may be contacted in an environment where their responses can be overheard by others. For example, a potential survey participant may be contacted while waiting in line at the bank or travelling

on public transit. If participants provide responses in such an environment, they may inadvertently disclose personal information to others within their vicinity. The survey respondents may also alter their responses or feel uncomfortable answering certain questions. When contacting potential survey participants via telephone, you should ensure that their location is one where it is safe for them to respond and where they feel comfortable responding to questions.

Most online survey tools have functionality that allows them to email potential survey participants on your behalf. Usually this is done to invite individuals to participate in the survey. The email typically contains a link to the survey and any required notices concerning the collection, use and disclosure of personal information.

However, it is not always necessary for an online survey tool to email potential survey participants on your behalf. If the survey data does not need to be linked or associated with individual email addresses, you could email the potential survey participants yourself through your institutional email account. This is important to consider in the case of online survey providers where you may have little or no control over whether changes are made to the terms-of-service agreement as well as where the survey data may reside. Although this approach may prevent you from knowing which participants responded to the survey and which did not, it would further mitigate the risks associated with using an online survey provider.

PROVIDING ASSURANCES OF CONFIDENTIALITY

To encourage them to participate in the research and to provide open and honest responses, researchers typically assure survey research participants that their responses will be kept confidential. However, as previously noted, not all of the information provided by survey participants (e.g., the views and opinions expressed by individuals in their professional capacity) will be considered to be personal information that is subject to the privacy protection provisions of the *Acts*. In addition, all records (i.e., personal information and general records) in the custody or under the control of an institution could be subject to an access request under the *Acts* or could be disclosed as required by law.

The only way to ensure complete confidentiality is to avoid collecting personal information altogether by conducting anonymous surveys. Where the research design, for one reason or another, requires that the survey data be linked to an individual, assurances of confidentiality should only be provided with the proviso that confidentiality is not absolute — that a disclosure of personal information may occur if required by law.

SECURITY OF ONLINE TRANSMISSION

When transmitted over the Internet, responses of potential survey participants may be intercepted and decoded by third parties. In general, there is little that can be done to prevent a computer's transmissions from being intercepted when using the Internet. However, measures are available to ensure that any intercepted data cannot be read, understood or used by a hacker or malicious individual. This will typically be done through encryption – a means of coding a message so that only the source and destination of the transmission will be able to understand it.

In the case of an online survey, the responses of potential survey participants will be transmitted between a website, on which the survey is hosted, and a web browser, which the survey participants use to access and interact with the survey. This communication takes place by means of the Hyper Text Transfer Protocol (HTTP), which is the basic data communications protocol for the Web. A widely supported means of encrypting HTTP communications is the cryptographic protocol of Transport Layer Security (TLS) or its predecessor, Secure Sockets Layer (SSL). When layered on top of TLS, HTTP communications are securely encrypted in the form of the Hyper Text Transfer Protocol Secure (HTTPS) protocol.

PROVIDING NOTICE OF COLLECTION

Unless the survey is conducted anonymously, notice of the collection of personal information must be provided at the time of the survey in compliance with sections 39(2)/29(2) of the *Acts*, unless a waiver has been obtained from the responsible minister under the provincial *Act*. The requirements for providing notice of collection are outlined in Stage 4.

OBTAINING INFORMED CONSENT

Participation in survey research should always be on a voluntary basis. Individuals should not be asked to participate without their informed consent. Regardless of whether the survey responses are anonymous or linked to an identifiable individual, potential participants should be provided with as much information about the survey as possible. For example, the information provided to potential research participants should include the following:

- when a third party is conducting the research, the name of the organization conducting the research and the name of the institution on whose behalf the research is being conducted;
- when an institution is conducting the research, the name of the institution;

- the purpose of the research and how the information will be used and/or disclosed;
- the safeguards being implemented to protect personal information;
- how much time will be involved;
- that participation is voluntary and non-response to specific items is acceptable; and
- how respondents will be informed about the survey results.

In addition, if the survey is not being done anonymously, individuals should be told why it will be necessary to link the survey responses to personal information (e.g., to link survey responses with information collected at another point in time or with information obtained from another source such as a client or customer database, or to follow up with participants on their specific responses to the survey).

COLLECTING PERSONAL INFORMATION FROM THIRD PARTIES

In most survey research, any personal information that is collected will be collected directly from the individual to whom it relates. However, it is possible that some research designs may require the collection of personal information from third parties such as family members, caregivers, social workers, co-workers, or employees' supervisors.

Sections 39(1)/29(1) of the *Acts* require that personal information be collected directly from the individual to whom it relates, unless certain circumstances listed in sections 39(1)/29(1) exist (e.g., where the individual authorizes another manner of collection, where another manner of collection is authorized by or under a statute, etc.). Thus, if you intend to collect personal information from someone other than the individual to whom it relates, you must have the authority to do so under sections 39(1)/29(1).

STAGE 6: DATA ANALYSIS

In analysing the data, the survey responses should only be used and disclosed for the purposes specified to the survey participants at the time of collection. Sections 41/31 of the *Acts* address the *use* of personal information. These sections state that an institution shall not use personal information in its custody or under its control except,

- where the person to whom the information relates has identified that information in particular and consented to its use;

- for the purpose for which it was obtained or compiled or for a consistent purpose; or
- for a purpose for which the information may be disclosed to the institution under sections 42/32 of the *Acts.*[19]

Sections 42(1)/32 of the *Acts* address *disclosure* of personal information and state that an institution shall not disclose personal information in its custody or under its control except in specific circumstances, including:

- where the person to whom the information relates has identified that information in particular and consented to its disclosure;
- for the purpose for which it was obtained or compiled or for a consistent purpose.

If you decide to use or disclose the survey responses for a secondary purpose not specified at the time of collection and the survey has not been conducted anonymously, obtain the individual's consent.

STAGE 7: REPORTING OF RESULTS

Survey results are generally reported as aggregate information, thus protecting the privacy of individual participants. However, in some cases a survey may result in small cells of information (i.e., where a small number of people is being represented) that could inadvertently identify or be used to identify an individual. For example, in an anonymous survey of institution employees, survey participants might be asked to specify their gender and employee category (e.g., executive, manager, supervisor, or staff). But if there is only one individual of a particular gender who falls within a particular employee category (e.g., female/executive), then that individual's responses will be easy to identify.

If it is known in advance that a survey could result in information that relates to a small number of individuals (i.e., small cells), the collection of personal information can be avoided by eliminating or combining those categories that include few individuals. In the above example, the size of the cells could be increased by eliminating gender categories or by combining executives and managers into a more general category. However, if the potential occurrence of small cells is not anticipated in advance and personal information is inadvertently collected, further use and disclosure of this information must be avoided by not reporting information relating to a small number of individuals

19 As stated above, note that the provincial *Act* provides that an educational institution may use personal information in its alumni records and a hospital may use personal information in its records for the purpose of its own fundraising activities, if the personal information is reasonably necessary for the fundraising activities, subject to additional requirements. See sections 41(1)(d), 41(2) and 41(3) of the provincial *Act*.

(e.g., fewer than five) or by combining categories after the fact to increase the cell size to an acceptably large number.

STAGE 8: DATA ARCHIVING

Institutions must consider how the survey data will be stored for future use, for how long and in what format it will be stored, and how it will eventually be disposed of. If the survey has not been done anonymously, there are certain requirements for retaining personal information specified in the *Acts*.

In addition to these requirements, whenever possible, all personal information should be replaced with a special code and stored separately from the survey responses. The survey responses should only be relinked to the personal information when it is necessary to do so for specific, defined purposes.

Government institutions must retain personal information that has been used for a period of time so as to afford the individual to whom it relates an opportunity to obtain access to it. Section 40(1) of the provincial *Act* together with section 5 of Regulation 460 and section 30(1) of the municipal *Act* together with section 5 of Regulation 823 set out the prescribed retention period. Records retention requirements may also be set out in other legislation, regulations or by-laws. All institutions need to consider whether additional records retention requirements apply to them.

In addition, government institutions are responsible for ensuring the security and confidentiality of personal information in their custody or control including the secure destruction of the personal information at the end of the applicable retention period. Section 4 of Regulation 460 of the provincial *Act* and section 3 of Regulation 823 of the municipal *Act* provide for this requirement and describe the kinds of safeguards that institutions must implement to fulfill this requirement. For additional guidance on the secure destruction of personal information, please see the IPC's Fact Sheet #10, "Secure Destruction of Personal Information."[20]

20 Available at: https://www.ipc.on.ca/images/Resources/fact-10-e.pdf.

CONCLUSION

Government institutions are more frequently undertaking survey research to elicit input on their programs and services. This paper has detailed the privacy considerations at each stage in the design and implementation of survey research projects and has recommended some best practices.

Collecting personal information from survey participants, and using previously collected personal information to obtain a survey research sample are the two central privacy considerations in survey research. With respect to the collection of personal information, we support the view that most survey research can be carried out anonymously and personally identifiable survey data is only required in limited and specific circumstances. With respect to the use of previously collected personal information, even where survey research is carried out anonymously, personal information may still be needed to obtain your survey sample. Thus, you will need to consider individual privacy and compliance with the *Acts* in most cases.

APPENDIX A: CHECKLIST OF BEST PRACTICES

	BEST PRACTICE	COMPLETE	IN PROGRESS	N/A	NOTES
STAGE 1: ISSUE DEFINITION					
1	Clearly define the issues you wish to address. This will help to limit the collection of information to that which is necessary to address the issues at hand.				
STAGE 2: RESEARCH DESIGN AND QUESTIONNAIRE DEVELOPMENT					
2	Where staff of your institution or another institution conduct the survey, prepare terms of reference setting out the requirements for the secure collection, retention, use, disclosure and disposal of personal information, in accordance with the *Acts* and regulations. (See Appendix B for a sample terms of reference).				
3	Where an external consultant or private company conducts the research, establish a contractual agreement to ensure that personal information is securely collected, retained, used, disclosed and disposed of, in accordance with the *Acts* and regulations. See the Office of the Chief Information and Privacy Officer's "Guidelines for the Protection of Information when Contracting for Services" for information on developing appropriate contractual agreements.				
4	Review either the terms of reference or the contractual agreement periodically during the survey and at the completion of it, to ensure that all conditions set out in either document have been fully complied with.				

	BEST PRACTICE	COMPLETE	IN PROGRESS	N/A	NOTES
5	Where staff of your institution use an online survey provider to conduct the survey, ensure that the provider's terms-of-service agreement and privacy policy allow for the secure collection, retention, use, disclosure and disposal of personal information in accordance with the *Acts*.				
6	If your survey research involves personal information, ensure that the terms of service between the online survey provider and the institution are not subject to change without the express written consent of your institution.				
7	If your survey research does not involve personal information, review the online survey provider's terms-of-service agreement and privacy policy periodically during the survey, at the completion of it, and while the survey information is stored by the provider, to ensure that the conditions set out in it have not changed or continue to comply with the *Acts*.				
8	Do not use an online survey provider that allows third parties to track survey participants.				
9	If the online survey provider's servers are based outside of Ontario or Canada, evaluate the risk this poses to the privacy and security of the survey data, taking into consideration the sensitivity of the information, the laws of the jurisdiction where the information is stored and the extent to which safeguards can be used to mitigate the risk, if any.				
10	When conducting a survey online, consider the option of self-hosting and whether you have the necessary technical resources to securely install, operate and maintain the survey software and data.				

	BEST PRACTICE	COMPLETE	IN PROGRESS	N/A	NOTES
11	Determine early in the design of your survey if it is necessary to collect personal information, as defined in the *Acts*. Consider conducting a PIA. If you are uncertain as to whether the information in question is personal information, contact your institution's Freedom of Information and Privacy Co-ordinator or a Policy Advisor at the Ministry of Government and Consumer Services. If personal information will be collected, you must comply with the privacy protection provisions of the *Acts*.				
12	If possible, design a survey so that the information collected does not identify and cannot be used, either alone or with other information, to identify an individual (i.e., an anonymous survey).				
13	When conducting an anonymous survey online, ensure that the hosting system does not link or associate with the survey data any information automatically passed to it from a survey participant's device or computer that may be used to identify the individual.				
14	When conducting an online survey that does not have a fixed sample of participants (i.e., where the survey may be taken by anyone), consider privacy-protective alternatives for improving the integrity of the survey results.				
15	If the survey cannot be carried out anonymously, design it so that all personal information is replaced with a special code that can only be used to link the survey data to personal information when it is necessary to do so (i.e., a coded survey).				

BEST PRACTICE	COMPLETE	IN PROGRESS	N/A	NOTES
16 When conducting a coded survey, be sure to: • inform potential participants about this procedure and its purpose; • retain the coded survey data separately from the personal information; and • limit the number of people who are able to relink the survey responses with the personal information to those individuals with a need-to-know for specific, defined purposes.				
17 When collecting personal information at the same time as the survey responses, for a purpose not directly related to the survey, keep the two types of information completely separate and implement measures to ensure compliance with the *Acts* in relation to the personal information collected.				
18 Determine whether you have the legal authority to collect the personal information required for the survey, under sections 38(2)/28(2) of the *Acts*.				
19 If you have the legal authority to collect the personal information required for the survey, limit the amount of personal information collected for the survey to what is strictly necessary.				
20 Select a survey research method that complements the degree of sensitivity of the information to be collected.				
STAGE 3: PRE–TESTING (FINE–TUNING) THE SURVEY				
21 Treat any personal information collected during the pre-test in the same manner as you would treat personal information collected through the survey.				

BEST PRACTICE	COMPLETE	IN PROGRESS	N/A	NOTES
STAGE 4: SAMPLE SELECTION				
22 Where you know in advance that customer or client information will be used to select a survey sample, provide notice of this use at the time of collection.				
23 Where you have not anticipated using personal information to select a survey sample at the time of collection, only use the information for this purpose if: • the individual consents to the use; or • the use is consistent with the purpose for which the information was obtained or compiled.				
24 Before collecting personal information indirectly from another institution or third party to obtain a survey research sample, ensure that you have the authority to do so under sections 39(1)/29(1) of the *Acts*.				
25 The inclusion of personal information in a public database does not necessarily mean that you have the authority to collect that information to select a survey sample. Before collecting personal information from a public database for this purpose, ensure that you have the authority to do so under sections 38(2)/28(2) of the *Acts*.				

BEST PRACTICE	COMPLETE	IN PROGRESS	N/A	NOTES
26 Before sharing data to select a survey sample, you must have legal authority to collect, use and/or disclose personal information for this purpose. If you do have legal authority, enter into a data sharing agreement as per the IPC's *Model Data Sharing Agreement*. Among other things, the agreement should stipulate that: • the institution conducting the survey must comply with sections 38(2)/28(2) of the *Acts* with respect to the authority to collect the personal information being shared; • if the party maintaining the personal information bank is an institution subject to one of the *Acts*, it must have the authority to use and disclose the personal information for this purpose, respectively, under sections 41/31 and 42/32 of the *Acts*.				
27 If possible, avoid collecting personal information to obtain a survey research sample, by having the institution or third party that maintains the personal information contact potential research participants directly on your behalf.				
28 Before using personal information to contact potential research participants on behalf of another institution or third party, assess whether you are authorized to use the information for this purpose, under sections 41/31 of the *Acts*.				
29 When using personal information to select a survey research sample, comply with the requirements for personal information banks set out under sections 44 to 46 of the provincial *Act*, or sections 34 and 35 of the municipal *Act*.				

BEST PRACTICE	COMPLETE	IN PROGRESS	N/A	NOTES
STAGE 5: DATA COLLECTION				
30 When contacting potential survey participants, take steps to protect their privacy by not disclosing to third parties the name of your institution or the reason for contacting the potential survey participants.				
31 When contacting potential survey participants via telephone, take steps to protect their privacy by ensuring that they are in an environment where it is safe to respond and where they feel comfortable responding to questions.				
32 When using an online survey, if the survey data does not need to be linked or associated with individual email addresses, you should consider emailing the potential survey participants yourself through your institutional email account.				
33 Unless the survey is done anonymously, provide assurances of confidentiality only with the proviso that confidentiality is not absolute — that a disclosure of personal information may occur if required by law.				
34 When the responses of survey participants are transmitted over the Internet, ensure that they are securely encrypted using a cryptographic protocol such as HTTPS.				
35 When collecting personal information to conduct a survey, provide notice of collection, in compliance with sections 39(2)/29(2) of the *Acts*, unless a waiver has been obtained from the responsible minister under the provincial *Act*.				

BEST PRACTICE	COMPLETE	IN PROGRESS	N/A	NOTES
36 Before collecting any information from potential survey participants, provide sufficient information about the research project and obtain informed consent.				
37 Whenever possible, collect personal information directly from the individual to whom it relates.				
38 In conducting a survey in which personal information is to be collected from someone other than the individual to whom it relates, ensure that you have the authority to do so under sections 39(1)/29(1) of the *Acts*.				
STAGE 6: DATA ANALYSIS				
39 Use and disclose personal information collected through the survey only for the purposes specified to the survey participants at the time of collection.				
40 Before using or disclosing personal information for a purpose not specified at the time of collection, obtain the individual's consent.				
STAGE 7: REPORTING OF RESULTS				
41 Report survey results as aggregate information.				
42 Do not report small cells of information, where a specific individual could be identified.				
STAGE 8: DATA ARCHIVING				
43 Whenever possible, replace personal information with a special code and store it separately from the survey responses.				

	BEST PRACTICE	COMPLETE	IN PROGRESS	N/A	NOTES
44	Retain personal information for the period prescribed in the *Acts* (i.e., section 40(1) of the provincial *Act* together with section 5 of Regulation 460/section 30(1) of the municipal *Act* together with section 5 of Regulation 823). All institutions need to consider whether additional records retention requirements apply to them.				
45	Keep personal information secure as prescribed in the regulations (i.e., section 4 of Regulation 460/section 3 of Regulation 823). When destruction or disposal is appropriate, follow the guidance set out in Fact Sheet #10, "Secure Destruction of Personal Information."				

APPENDIX B: SAMPLE TERMS OF REFERENCE

Whenever staff of an institution conduct survey research, Terms of Reference should set out the requirements for the secure collection, retention, use, disclosure and disposal of personal information, in accordance with the *Acts*. A sample Terms of Reference for a municipal institution is found below.

TERMS OF REFERENCE

(Preamble describing events leading up to the survey, the survey itself, etc.)

- The purpose of this survey is to _____ .
- The staff responsible for conducting the survey are _____ .
- The staff conducting the survey shall comply with the provisions of the *Municipal Freedom of Information and Protection of Privacy Act*, and its regulations, in the course of conducting the survey.
- The staff conducting the survey will use and/or disclose the data, information, reports, material or other documents of any nature which are disclosed, revealed or transmitted to them, or to which they have access, solely for the purpose of conducting the survey.
- Staff will collect, use or disclose only the minimal amount of personal information necessary to conduct the survey.
- When personal information is collected, staff shall provide the survey respondents with proper notice of collection, in accordance with section 29(2) of the *Municipal Freedom of Information and Protection of Privacy Act*.
- Staff will ensure that personal information used during the survey shall be retained in accordance with section 30(1) of the *Municipal Freedom of Information and Protection of Privacy Act* together with section 5 of Regulation 823.
- Staff will ensure that any personal information to be disposed of upon completion of the survey, is done so in accordance with the disposal procedures outlined in *IPC Practice 26*, *Safe and Secure Disposal Procedures for Municipal Institutions*.
- Staff shall keep all information involved in the survey secure and confidential.

For more information, contact: _____

.

ABOUT THE INFORMATION AND PRIVACY COMMISSIONER OF ONTARIO

The role of the Information and Privacy Commissioner of Ontario is set out in three statutes: the *Freedom of Information and Protection of Privacy Act*, the *Municipal Freedom of Information and Protection of Privacy Act* and the *Personal Health Information Protection Act*. The Commissioner acts independently of government to uphold and promote open government and the protection of personal privacy.

Under the three *Acts*, the Commissioner:

- **Resolves access to information appeals and complaints when government or health care practitioners and organizations refuse to grant requests for access or correction;**
- **Investigates complaints with respect to personal information held by government or health care practitioners and organizations;**
- **Conducts research into access and privacy issues;**
- **Comments on proposed government legislation and programs; and**
- **Educates the public about Ontario's access and privacy laws.**

Information and Privacy
Commissioner of Ontario

Commissaire à l'information et à la
protection de la vie privée de l'Ontario

Information and Privacy Commissioner of Ontario
2 Bloor Street East, Suite 1400
Toronto, Ontario
Canada M4W 1A8

Web site: www.ipc.on.ca
Telephone: 416-326-3333
Email: info@ipc.on.ca

April 2015