Privacy Impact Assessment Guidelines

Ministry of

Privacy and Legislation Branch,
Office of the Chief Information Officer

May, 2014
What is a Privacy Impact Assessment (PIA)?

A PIA is an assessment tool used to evaluate privacy impacts, including compliance with the privacy protection responsibilities under FOIPPA. PIAs promote transparency and accountability, and contribute to continued public confidence in the way government manages personal information.

Why do I need to complete a PIA?

Completing a PIA is a legislative requirement. Section 69(5) of FOIPPA requires the head of a ministry to conduct a PIA in accordance with the directions of the minister responsible for FOIPPA.

Section 69(5.1) requires PIAs to be submitted to the minister responsible for FOIPPA for review and comment during the development of any proposed enactment, system, project, program or activity—from now on referred to generally as an “initiative”. A PIA must also be submitted during the development of any proposed updates to a current initiative.

The Privacy and Legislation Branch (PLB) is the representative of the minister for the purpose of PIAs. Ministries must submit a PIA to PLB at pia.intake@gov.bc.ca for review and comment prior to the implementation of any initiative or any proposed revisions to an initiative. Further information can be found on the Useful Resources page of these guidelines.

Note: There are several PIA templates available for use depending on the nature of the initiative that is subject to the assessment being conducted.

However, these guidelines are for the General PIA Template only, which can be found on the PLB website (see the Useful Resources on page 18 of these guidelines for a link to the General PIA template).
What is personal information?

FOIPPA provides a simple but broad definition of personal information:

“Recorded information about an identifiable individual other than contact information.”

Note: contact information is information used to contact someone at a place of business.

The following is a non-exhaustive list of personal information examples:

- name, address, email address, or telephone number;
- age, sex, religious beliefs, sexual orientation, marital or family status, blood type;
- an identifying number, symbol or other particular assigned to an individual;
- information about an individual’s health care history, including a physical or mental disability;
- information about an individual’s educational, financial, criminal or employment history; and
- personal views or opinions.

It is important to note that personal information includes information that can be combined with other information to identify a specific individual, even through association or inference. For example, if information such as ethnic origin were linked to health information and only one person in a small town was of that ethnic origin, this could potentially reveal sensitive health information about that person.

What if my initiative does not include personal information?

Ministries must complete and submit a PIA to PLB even if it is thought that no personal information is involved. This allows PLB to ensure the initiative has been accurately assessed. If the initiative does not appear to involve personal information, a program area needs to only fill out Part 1 of the PIA before submitting it unsigned to PLB.

An initiative assessed by PLB not to involve personal information can be signed (when directed to sign by PLB) by an Executive Director (or equivalent) as opposed to an ADM or designate.
PLB Timelines

A standard PIA takes approximately three weeks to be reviewed and signed by PLB. However, timelines get longer when more information is needed.

Of course, all initiatives are different and so are their PIAs. If your initiative is a cross-government, multi-phase/multi component project, you may need multiple PIAs to address the project’s complexities. On the other hand, if you are merely collecting survey data it may take only a day to complete your PIA. Check with PLB if you have any questions about a PIA timeline.

Tip: Get your PIA into PLB at the beginning of your planning stages. You may not yet have everything figured out, but your assigned PLB Privacy Advisor will be able to point out privacy implications at the onset of your initiative. This increases the likelihood of avoiding subsequent problems.

Things needed to complete a PIA

Before jumping into writing your PIA, there are a few things you may want to collect first:

- any relevant/previous PIAs already completed around this initiative;
- any legislation, other than FOIPPA, relevant to your initiative;
- information about where your data is stored, accessed, and where it flows;
- security information about the data—i.e., do you need to contact your Ministry Information Security Officer? (see page 13);
- any records retention schedules for your initiative—i.e., do you need to contact your Ministry Records Officer?
- any relevant Research Agreement(s);
- Information about any materials required to obtain program manager’s and ADM’s/Executive Director’s signatures.
Question 1 asks you to describe the system, project, program or activity that is the subject of the PIA. Whether you’re building a new system for your ministry or setting up a new social media page, you want to give as much relevant detail as possible about your initiative.

When answering this question, be as precise, clear and concise as possible. Remember, your audience will not be familiar with the initiative and may not have any related background knowledge. Try to contextualize your initiative by thinking about the “who, what, where, when, why and how” questions:

**What** is the initiative? - Is it an effort to improve services to citizens or a way to streamline government processes?

**Who** is involved in this initiative? - Is it just one ministry or is it between two ministries and a private sector organization?

**Where** is the initiative taking place? - Is it online, in person or paper-based?

**When** is the initiative occurring? - Is this a revision to an ongoing initiative or a new initiative that will commence in 6 months?

**Why** is the initiative happening? - Is it fulfilling a legislative requirement or trying to meet demands for online service delivery?

**How** is the initiative being implemented? Are two ministries collaborating via SharePoint or creating a new website?

**Question 2**, in asking about the scope of the PIA, is trying to provide clarity and focus about what is being assessed in the PIA. This is particularly important when your initiative has multiple aspects or phases. For example, the PIA may only address one particular aspect of the initiative.

This section should clearly articulate exactly what the PIA covers. For example, if the
description provides details about a Ministry’s overhaul of its citizen engagement policy and its focus on launching new communication tools, it is important to note in the scope section that this PIA is only about its “new blog” or about “phase 3” of the project.

**Question 3** asks if there have been previous PIAs that were conducted on your project. It may speed up the review process if you provide us with these previous or related PIAs. They can help your assigned privacy advisor get a better understanding of your project and any privacy reviews already conducted.

**Question 4** asks you to list all the elements of information and data included in your initiative, not just personal information. This is an important step, as it allows a Privacy Advisor to assess all of the information involved against what FOIPPA considers to be “personal information” and helps to set the foundation for the remainder of the PIA review.

For example, if you are conducting a survey, you may want to list the different elements of personal information for which you ask, and provide a summary of the other types of questions. A summary may include things like: questions about respondent’s feelings on your program delivery.

If you believe your initiative does not contain personal information, completed PIAs can be submitted (unsigned) containing only Part 1. PIAs can be sent to PIA.intake@gov.bc.ca.

**Question 5** asks for details about the storage and access of personal information because FOIPPA only permits personal information from being stored outside of Canada or accessed from outside of Canada in limited circumstances. It is important for us to know where your information is being stored, whether in a Kelowna secure facility or “out there in the cloud.” The same goes for access: where are the people who have access to your data located? Are they all within Canada or do they travel abroad and remotely access the data? Similarly, when something goes wrong with your system, are issues resolved by a Canadian company or technician, or by experts from another country?

**Question 6** asks you to identify whether or not your initiative is a “data-linking initiative”. In order to answer this question it is necessary to know how FOIPPA defines the terms “data linking” and “data-linking initiative.”
“Data linking” is defined as: “the linking or combining of personal information in one database with personal information in one or more other databases if the purpose of the linking or combining is different from:

(a) the purpose for which the information in each database was originally obtained or compiled, and
(b) every purpose that is consistent with each purpose referred to in paragraph (a)”.

A “data-linking initiative” is defined as: “a new or newly revised enactment, system, project, program or activity that has, as a component, data linking between

(a) two or more public bodies, or
(b) one or more public bodies and one or more agencies.”

Data-Linking Assessment:

If, based on the definitions above, or the three “yes/no” questions in question 6 of the PIA, you think that you might have a data-linking initiative, you should refer to the more detailed flow diagram (appendix A of these Guidelines) that sets out the more specific criteria around data-linking initiatives. This flow chart will be helpful in assessing whether or not you meet all the criteria.

If you are still unsure whether your initiative is a data-linking initiative, please contact your PLB Privacy Advisor for assistance.

Stop! Has the Office of the Information and Privacy Commissioner (OIPC) been notified?
Section 69(5.5) of FOIPPA requires ministries to notify the OIPC of a data-linking initiative in the early stages of developing the initiative. If ministries have a data-linking initiative, PLB can facilitate the notification of the OIPC.

Question 7 asks you to identify whether or not your initiative is a “common or integrated program or activity”. FOIPPA defines ‘common or integrated program or activity” as: “a program or activity that:

(a) provides one or more services through
   (i) a public body and one or more other public bodies or agencies working
collaboratively, or

(ii) one public body working on behalf of one or more other public bodies or agencies, and

(b) is confirmed by regulation as being a common or integrated program or activity.”

To be “confirmed by regulation” means that you have developed the written documentation that meets the requirements of s.12 of the FOIPP Regulation. This is commonly referred to as a Integrated Program Agreement (IPA).

If you answer “yes” to the three questions set out in question 7 of the PIA, then yours is a common or integrated program or activity. If you answer “no” to just one of these, then yours is not a common or integrated program or activity.

If you are still unsure if your initiative is a common or integrated program or activity, please contact your PLB Privacy Advisor for assistance.

Stop! Has the Office of the Information and Privacy Commissioner (OIPC) been notified?
Section 69(5.5) of FOIPPA requires ministries to notify the OIPC of a common or integrated program or activity in the early stages of developing the program or activity. If ministries are confirmed as having a common or integrated program or activity, PLB can facilitate the notification of the OIPC.

The Office of the Information and Privacy Commissioner (OIPC)

The OIPC is an independent agency mandated to oversee and enforce compliance with FOIPPA. Among other duties set out in FOIPPA, the Commissioner’s Office must review and comment on all PIAs that involve a data-linking initiative or a common or integrated program or activity. It is important to note that the OIPC provides guidance on how to bring your program into compliance but does not approve, endorse, or sign off on your PIA.

You can learn more about the OIPC at their website: www.oipc.bc.ca
Part 2 of the PIA gets into the specifics of government’s duty to protect personal information in its custody and/or control. If your initiative is dealing with personal information you will need to complete the remainder of the PIA. It is important that the answers you provide here are accurate to ensure that government remains compliant with legislation.

**Question 8** asks for a flow diagram or flow table that shows how your initiative will collect, use, and/or disclose personal information. It should also outline the flows of personal information wherever it is transmitted or exchanged. It is quite easy to create a flow diagram: if you have Microsoft Visio on your computer, you can quickly create a diagram that might look something like this:
Or this:

Your diagram and/or table must also include the authorities for the collection, use, and/or disclosure of personal information, as laid out in FOIPPA. If you don’t know the authorities, refer to the PIA appendices (links provided on pg. 18) or ask your PLB Privacy Advisor.

Of course, you don’t need Microsoft Visio to create a simple diagram that allows readers to easily understand the flows of information. With Microsoft Word, for example, you could create simple flow diagrams.

One of the simplest applications to use for diagrams is PowerPoint. You can quickly and easily create a flow diagram on a slide, and then save it as a .jpeg file to put into your PIA. For those not technically inclined, hand drawn images can also be scanned and inserted into the PIA.
For those who would prefer to write their processes out, or for whom a diagram does not make sense, an information flow table is an easy and effective way to convey the same information.

The PIA template provides an example of an information flow table from which you can work. Simply remove the examples and fill them in with your own.

<table>
<thead>
<tr>
<th>Description/Purpose</th>
<th>Type</th>
<th>Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Email received from client requesting service</td>
<td>Collection</td>
<td>26(c)</td>
</tr>
<tr>
<td>2. Email client back requesting more information</td>
<td>Disclosure</td>
<td>33.1(7)</td>
</tr>
<tr>
<td>3. Service request transferred to service provider contracted by Ministry</td>
<td>Disclosure &amp; Use</td>
<td>33.2(c) and 32(a)</td>
</tr>
<tr>
<td>4.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The key to an effective information flow table is to break down your initiative into its most basic parts. Explain the way information moves through your initiative as if you were explaining it to someone who doesn’t work for government and isn’t familiar with what you do.

Focus should be given to when you are either collecting information from someone/somewhere, whenever you are using the personal information and when you are disclosing or sharing information with someone/somewhere else.

Examples of potential personal information collection:

- Application or submission forms;
- Comment boxes or web postings;
- Consultations and surveys;
- Analytics;
- Receiving information about an individual from another program area.

You do not have to be collecting information directly from an individual for it to be considered collection. For example, if a ministry collects personal information from another ministry as opposed to from the person it is about, the ministry is collecting this personal information ‘indirectly’. You will require an additional authority in order to collect personal information indirectly. These authorities can be found in s.27(1) of FOIPPA or in the appendices to the PIA.
In your flow diagram or table, you should also describe when your initiative uses personal information that has been collected or is already in your possession. For example, if your initiative provides government grants and you have collected personal information from clients as part of that initiative, that information might be used for issuing grants and for evaluating geographic distribution of grant allocation. These two separate “uses” should be documented in your flow diagram or table.

Examples of potential personal information disclosures:

- Transferring information to or sharing information with another program area;
- Publishing information in print or online (or allowing people to post publicly to your website);
- Verifying information for another program area;
- Providing information upon request (e.g. from police, citizens, a ministry, etc.).

**Question 9** asks for a risk mitigation table to identify any potential privacy risks that your initiative may have and how you intend to manage, mitigate or eliminate those risks. An example of a risk mitigation table is provided below:

<table>
<thead>
<tr>
<th>Risk</th>
<th>Mitigation Strategy</th>
<th>Likelihood</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Employees could access personal information and use or disclose it for personal purposes</td>
<td>Oath of Employment</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Request may not actually be from client (i.e. their email address may be being used by someone else)</td>
<td>Implementation of identification verification procedures</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Client’s personal information is compromised when transferred to the service provider</td>
<td>Transmission is encrypted and over a secure line</td>
<td>Low</td>
<td>High</td>
</tr>
<tr>
<td>Inherent risks in sending personal information to a client via email</td>
<td>Policy developed to inform clients of risk and ask if they would like the information via a different medium, such as through the mail</td>
<td>Medium</td>
<td>Medium</td>
</tr>
</tbody>
</table>
contraventions of FOIPPA, such as storage outside of Canada. Think about vulnerabilities or places where the personal information might be accessed by someone who should not have access. Is there a possibility you could receive more information than you asked for or want? Essentially, a risk is anything that falls outside of the mantra “right information, right person, right purpose, right time, right way.”

Once you have identified any privacy risks or harms, you must plan how to manage, mitigate or eliminate them. For each risk or harm identified you will also have to estimate the likelihood of the risk occurring and what the impact would be if the risk materialized.

**If you aren’t sure how certain risks might be managed, mitigated or eliminated, this might be a good time to check in with your PLB Privacy Advisor.**

There are many factors that can affect the likelihood or impact of a risk, and these factors all have to be weighed in the assessment. Use the tables found in Appendices B and C to gain a general sense of how different factors may influence the risk’s impact or potential likelihood.

**Question 10** should be used to document your collection notification details. Section 27(2) of FOIPPA requires that the individual from whom personal information is being collected be provided specific information about the collection. The following sample collection notification illustrates this information:

```
Sample notification for collection:

This information is collected by [name of public body] under [section] of the [name of enactment] and will be used to [purpose]. Should you have any questions about the collection of this personal information please contact

[Position Title]
[Address]
[Phone Number]
```

There are instances where a collection notification would not be required. These exceptions are set out in section 27(3) of FOIPPA. You can also refer to the PIA appendices if you do not know what the exceptions are.
Whenever a public body collects, uses, discloses, stores or disposes of personal information, it must make reasonable arrangements to protect that personal information. This means protecting it when it is at rest (e.g. on a desktop computer) and in transit (e.g. when being disclosed to another public body or third party).

Questions 11 and 12 should be used to describe any and all security measures you have in place. This may be technical security such as passwords and firewalls, or physical measures such as locked cabinets and secure physical sign-in to buildings.

Question 13 asks if you rely on security policies in addition to the Information Security Policy. You should indicate the local policies and procedures being used for the protection of information. For example, you may also be using specific branch-developed procedures to protect data (e.g. employees in your branch may not be permitted to access certain data remotely).

Access to personal information should be restricted to those employees who need the information in order to carry out their roles and responsibilities. In many cases there should be systems in place that track who has accessed information, when it was accessed, for how long it was accessed, and what uses of, or changes to, the information have been made.

Questions 14 and 15 require that you explain how an individual accessing personal information without authorization will be identified. Similarly, explain the ways in which this unauthorized access will be prevented or mitigated.

If your initiative involves an information system, or if it is otherwise deemed necessary to do so, you may need to consult with your Ministry Information Security Officer (MISO) to help you fill out the security section of the PIA. Your MISO will also be able to tell you whether you will need to complete a separate assessment called a Security Threat and Risk Assessment (STRA) for your initiative.
If personal information is used by a public body to make a decision that directly affects that individual, the public body must make every reasonable effort to ensure that the personal information is accurate and complete.

**Question 16** asks 3 interrelated questions that relate to ensuring the accuracy of personal information. FOIPPA requires that public bodies have a plan in place to address an individual’s request to update or correct their personal information.

Individuals have a right to request a correction to their personal information if they believe it is wrong or incomplete. If an individual makes a request for correction but no correction is made, the ministry must annotate the information with the requested correction.

Finally, following the correction (or annotation), the ministry must notify those to whom they have previously disclosed the personal information so that the personal information held by others is also accurate and complete.

If an individual contacts your ministry and asks that their personal information be corrected, how would you go about correcting it? This is essentially what question 16 is asking. Is the individual able to correct/update their own information online? Will the public body clearly mark the original information as incorrect and attach the correct information to the file? Similarly, if personal information cannot be corrected, how will it be annotated with the correction that was requested but not made?

Finally, what steps will be taken to notify other holders of the personal information of the correction/annotation? Will they be notified on an ad hoc basis if and when a correction or

---

**Accuracy, Correction and Retention of Personal Information — Part 4 of the PIA**

To "annotate" means to add explanatory notes to a record such as a letter, report or other document (e.g., a letter or written statement in which the applicant disputes the facts as presented or disagrees with an opinion expressed by another person about the applicant).
annotation is made, or, if public bodies are sharing personal information on a regular and systematic basis, will the updates be similarly regular and systematic?

**Question 17** refers to a "decision", which in this context means a conclusion, formal judgment (including the reasons which were used in reaching that judgment), or resolution that, in some manner, directly affects the individual concerned.

For example, if an individual’s date of birth is used to determine their entitlement to a benefit or service, then that individual’s personal information has been used to make a decision that directly affects them (i.e. whether or not they receive that benefit or service).

**Question 18** asks for what measures you will take to ensure the accuracy and completeness of personal information. This could include error-proofing of forms, manually verifying information before decisions are made or periodic checks of databases.

**Question 19** recognizes that individuals must be given a reasonable opportunity to access personal information that has been used by the ministry to make a decision that directly affects them. This allows the individual an opportunity to review the information, and if necessary, request a correction. Therefore, ministries are required to retain that personal information for at least one year after it was used to make the decision.

Sometimes personal information needs to be kept longer than one year, depending on operational needs. However, personal information should not be retained indefinitely as this increases the potential for out-of-date or incomplete information and also increases the risk of an unauthorized access or disclosure. In all cases, government records must be disposed of securely in accordance with approved records retention/disposition schedules.

If you have applied for a records retention schedule and are waiting for it to be in place, you should explain in this question how those records will be kept in the interim.
Question 20 is asking if your initiative shares personal information systematically, i.e. according to a fixed plan and on a regular (as opposed to an ad hoc) basis. If this is true of your initiative, use this section to explain from whom or to whom the personal information is being routinely or systematically collected or disclosed and for what purpose.

If you answer “yes” to question 20, you will need to indicate that you have prepared an Information Sharing Agreement. For general questions on ISAs you can speak to your PLB Privacy advisor or contact the Privacy and Access Helpline (see Useful Resources page of these Guidelines).

If an ISA has been prepared as part of your initiative, please complete the table below question 20. Providing this information is required under s. 69(4) of FOIPPA. As also required by FOIPPA, this information will be posted on DataBC in the Personal Information Directory.

Question 21 asks you to indicate whether or not the personal information involved in your initiative (or parts of it) are going to be disclosed to researchers for research purposes. If this is true of your initiative, use this section to explain what personal information will be disclosed and the purposes for which it will be used.

If you answer “yes” to question 21, you will need to indicate that you have completed a Research Agreement and that it is attached to your PIA.

If you answered “yes” to question 21, but you haven’t completed a Research Agreement, please talk to your PLB Privacy Advisor about how to complete one and where to find the approved template.

Question 22 refers to a Personal Information Bank (PIB), which is a collection of personal information organized or retrievable by the name of an individual or by an identifying number, symbol or other particular assigned to an individual. If you believe that your initiative will result in a PIB, use this question to flesh out some of the details as to what that PIB will entail. For example, what types of personal information are included (e.g. financial, health related, legal, etc.)

Providing this information is required under s. 69(4) of FOIPPA. As also required by FOIPPA, this information will be posted on DataBC in the Personal Information Directory.
How do I submit my PIA?

PIAs should be submitted to PLB at the beginning of your planning stages. You may not yet have everything figured out, but your assigned PLB Privacy Advisor will be able to point out privacy implications at the onset of your initiative. This increases the likelihood of avoiding subsequent problems.

PIAs should be submitted to PLB before the sign-off process is started. Submissions can be made to PIA.Intake@gov.bc.ca. You will be assigned a Privacy Advisor within a day or two.

What if I've already conducted a PIA and I'm only making changes to an existing initiative?

If you are only making changes to an existing initiative (for which a PIA has already been conducted), you may be able to complete an Initiative Update PIA, which is a targeted PIA Template specifically designed to only assess changes to an existing initiative. See the Useful Resources page of these guidelines for a link to the Initiative Update PIA template.

What is a Security Threat and Risk Assessment (STRA)?

A STRA is a risk management process designed to identify business risks associated with information systems and technology. The assessment process helps define how critical the information is to a business, and then identify issues and control gaps that would result in a business impact, such as a privacy or security breach. The completion of an STRA is a requirement for all government information systems. See the Useful Resources page of these guidelines for contact information regarding the Security Threat and Risk Assessment process.

What is a Ministry Information Security Officer (MISO)?

A MISO is the person within your ministry responsible for information security. MISOs can sign off on the security of your program once they have assessed how well it meets minimum security standards. This might mean conducting a STRA, or simply providing detailed information about how information will be managed.
Help: Who to Contact for Assistance

If at anytime you have any questions regarding access, privacy or the PIA process, please contact PLB’s helpline:

- Email: privacy.helpline@gov.bc.ca
- Phone: 250-356-1851, or 1-800-663-7867 (and ask for the Privacy and Access Helpline).

Useful Resources

- Privacy and Legislation Branch website: http://www.cio.gov.bc.ca/cio/priv_leg/LPP.page?
- Directory of Ministry Information Security Officers (MISOs) *An IDIR is required to access this page: https://www.cio.gov.bc.ca/MISO/MISOs.htm
- Information Security Branch (for questions on STRAs): CITZCIOSecurity@gov.bc.ca
- Directory of Ministry Records Officers: http://www.gov.bc.ca/citz/iao/records_mgmt/contact_us/ministry_records_officers.html
- General PIA template and appendices: http://www.cio.gov.bc.ca/cio/priv_leg/foippa/pia/pia_index.page?
- PIA Directions to government ministries: http://www.cio.gov.bc.ca/cio/priv_leg/foippa/pia/pia_index.page?
- Office of the Information and Privacy Commissioner (OIPC) website: http://www.oipc.bc.ca/
Appendix A
Data Linking Assessment Chart

START:

Are all the participants in your data-linking initiative a health care body, the Ministry of Health or a health-related organization as prescribed? Yes  
No

Does your initiative involve the linking or combining (whether temporary or permanent) of personal information in one database with personal information in one or more other databases? Yes
No

Does the linking of personal information occur between two or more public bodies or between one or more public bodies and one or more agencies? Yes
No

Is the purpose of the linking of personal information different from the purpose for which the information in each database was originally obtained or compiled, and every purpose that is consistent* with these purposes? Yes  
No

Was the initiative implemented after November 14, 2011? Yes  
No

Before November 14, 2011, had your public body completed a written project plan respecting the data-linking initiative that meets the criteria set out in s.36.1(4) of FOIPPA? Yes
No

Is your initiative an existing data-linking initiative being expanded by doing any of the things set out in s.36.1(3) of FOIPPA? Yes
No

END: Your initiative is NOT a data-linking initiative subject to the FOIPP Regulations

Yes
No

END: Your initiative is a data-linking initiative and must comply with the FOIPP Regulations

Yes
No

* A use of personal information is consistent with the purpose for which the information was obtained or compiled if the use
 a) Has a reasonable and direct connection to that purpose, and
 b) Is necessary for performing the statutory duties of, or for operating a program or activity of, the public body that uses or discloses the information.
All factors identified in the impact table can, under certain circumstances, become higher or lower impact. For example, low risk personal information in one situation can become high risk in another if there are factors that change how the individual will be affected.

<table>
<thead>
<tr>
<th>“Impact” Factors Guidance Table</th>
<th>Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Factors affecting the impact of a risk</td>
<td>High</td>
</tr>
<tr>
<td>1. Sensitivity of personal information</td>
<td>Identity information, financial information, biometrics, health information</td>
</tr>
<tr>
<td>2. Mosaic effect of information (can be combined with other information that is publicly available to identify individuals)</td>
<td>Very small population or geographic area, very unique characteristics (e.g., small town in B.C.)</td>
</tr>
<tr>
<td>3. Effect on individuals or third parties</td>
<td>Risk of identity theft, physical harm, hurt or humiliation, or risk to business opportunities</td>
</tr>
<tr>
<td>4. Audience of unauthorized disclosures</td>
<td>101+ people</td>
</tr>
<tr>
<td>5. Effect on Government’s credibility or reputation</td>
<td>Bad press, political ramifications, public outcry</td>
</tr>
</tbody>
</table>
All factors identified in the Likelihood table can, under certain circumstances, become higher or lower likelihood. For example, low risk personal information in one situation can become high risk in another if there are factors that change how the individual will be affected.

<table>
<thead>
<tr>
<th>“Likelihood” Factors Guidance Table</th>
<th>Likelihood</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Factors affecting the likelihood of a risk materializing</strong></td>
<td>High</td>
</tr>
<tr>
<td>1. Content is public-facing</td>
<td>No moderation or monitoring of content</td>
</tr>
<tr>
<td>2. Group access to content</td>
<td>Open access</td>
</tr>
<tr>
<td>3. Technical security measures</td>
<td>No encryption, no password protection.</td>
</tr>
<tr>
<td>5. Policy</td>
<td>No access policies, no clear-set guidelines regarding information management. No education of existing policies.</td>
</tr>
</tbody>
</table>