# STEP 3 |PRIVACY ANALYSIS

## PART 1: Collection, use, and disclosure

The following tables will ask a series of questions to assist organizations in determining if it is in compliance with the legislation. These following tables will deal with the:

- Collection,
- Use,
- Disclosure.

> **Collection** occurs when a public body gathers, acquires, receives or obtains PI/PHI.
>
> **Use** indicates the internal utilization of PI/PHI by a public body and includes sharing of the PI/PHI in such a way that it remains under the control of that public body.
>
> **Disclosure** is the sharing of PI/PHI with a separate entity, not a division or branch of the public body in possession or control of the PI/PHI.

The tables will also ask about safeguards that organizations can put into place to protect PI/PHI.

> Examples of **administrative safeguards** include policies, procedures, agreements, contracts, training resources.

Examples of **technical safeguards** include protecting information through strong passwords and encryption, automatic log off features for computers (after a short time of user inactivity), and firewalls.

Examples of **physical safeguards** include locked filing cabinets, restricted access to areas containing personal information/personal health information, computer monitor privacy screens, and alarm systems.

If a visualization of the project was created in Step 2, it can be used to help with identifying where PI/PHI is collected, used, and disclosed. The tables below will assist in determining whether there is authority for each flow of PI/PHI. **The questions in the table should be applied to each flow of PI/PHI identified in the visualizations. If the flow deals with collection, then the collection table should be filled out. If the flow of the PI/PHI deals with use, then the use table should be filled out. If the flow of the PI/PHI deals with disclose, then the disclosure table should be filled out.**

### A. Collection

| Privacy Requirement Questions | Yes | No | Unknown | Explanation | Privacy Impact | Action Items |
|---|---|---|---|---|---|---|
| **Name of Flow (example: Flow #1, Flow #2, etc.)** | | | | | | |
| **Authority for flow (example: FOIP, LA FOIP, HIPA)** | | | | | | |
| Does the legislation authorize the collection of PI/PHI? | | | | | | |
| Is there legislation besides FOIP, LA FOIP, and/or HIPA that addresses the collection of PI/PHI? | | | | | | |
| **Purpose of Collection** | | | | | | |
| Has the purpose of the collection been defined? What is the | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| purpose of the collection? | | | | | | |
| **Notice to Individual** | | | | | | |
| Will notice of collection be given to the individual(s)? Explain timing, method of notification.<br><br>If notice won't be given to the individual, give reasons and explain why the lack of notice is in compliance with subsection 26(3) of FOIP, 25(3) of LA FOIP, or 25(1)(c) of HIPA. | | | | | | |
| **Manner of Collection** | | | | | | |
| Will PI/PHI be collected directly from the individual? | | | | | | |
| Will p PI/PHI be collected indirectly from another source? If so, explain the authority for the indirect collection. | | | | | | |
| **Data Minimization** | | | | | | |
| Is the project only collecting those pieces of PI/PHI it requires to achieve the project's purpose? | | | | | | |
| What controls are in place to ensure the project only collects | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| the information it requires? (Examples: Forms that asks for the PI/PHI hat is required, processes are in place to return extra PI/PHI that was collected, etc.) | | | | | | |
| **SAFEGUARDS** | | | | | | |
| Are there administrative safeguards in place to ensure only the PI/PHI that is required for the project is being collected? (Examples: Forms that only ask for the PI/PHI that is needed; policies, procedures, and training are in place so staff know what PI/PHI is to be collected. Attach copies of the policies, procedures and training material). | | | | | | |
| Are there technical safeguards in place to ensure only the PI/PHI that is required for the project is being collected? (Examples: Forms that only ask for the PI/PHI that is needed.) | | | | | | |
| Are there physical safeguards in place to ensure only the PI/PHI that is required for the project is being collected? | | | | | | |

**B. USE**

| Privacy Requirement Questions | Yes | No | Unknown | Explanation | Privacy Impact | Action Items |
|---|---|---|---|---|---|---|
| **Name of Flow (example: Flow #1, Flow #2, etc.)** | | | | | | |
| **Authority for Flow (example: FOIP, LA FOIP, HIPA)** | | | | | | |
| Does the legislation authorize the use of the PI/PHI? | | | | | | |
| Is there legislation besides FOIP, LA FOIP, HIPA that addresses the use of PI/PHI? | | | | | | |
| **Purpose** | | | | | | |
| Will the PI/PHI be used for the same purpose as the collection of PI/PHI? | | | | | | |
| Will the PI/PHI be used for a purpose that is consistent with the purpose for the collection of PI/PHI? | | | | | | |
| Will the PI/PHI be used for a secondary purpose? (ie, a purpose that is not the same as the purpose for the collection of | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| PI/PHI). If so, please explain the authority for the secondary purpose. | | | | | | |
| **Standard of Accuracy** | | | | | | |
| Are there procedures in place so that your organization can verify that it has the most accurate and complete PI/PHI of an individual that it needs? | | | | | | |
| Are there procedures in place so that individuals are able to request that their PI/PHI is corrected? | | | | | | |
| **Safeguards** | | | | | | |
| Are there administrative safeguards in place to ensure that PI/PHI will be used only for authorized purposes? (Examples: Policies, procedures, and training are in place so staff know how PI/PHI is to be used. Attach copies of the policies, procedures and training material). | | | | | | |
| Are there technical safeguards in place to ensure PI/PHI will be used only for authorized purposes? | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| (Example: staff are only given access to parts of databases that contains PI/PHI it needs to complete job duties; documents can be encrypted and/or password protected to ensure only intended recipients can open the documents; audits are completed to ensure staff only accessing PI/PHI it needs for job duties, etc.) | | | | | | |
| Are there physical safeguards in place to ensure PI/PHI is used for authorized purposes? (Example: Only staff who require PI/PHI are given physical access to areas where PI/PHI is stored such as records rooms, filing cabinets, etc.). | | | | | | |

**C. DISCLOSURE**

| Privacy Requirement Questions | Yes | No | Unknown | Explanation | Privacy Impact | Action Items |
|---|---|---|---|---|---|---|
| **Name of Flow (example: Flow #1, Flow #2, etc.)** | | | | | | |
| **Authority for Flow (example: FOIP, LA FOIP, HIPA)** | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| What is the authority for the disclosure of PI/PHI? | | | | | | |
| **Safeguards** | | | | | | |
| Are there administrative safeguards in place to ensure only the PI/PHI that needs to be disclosed is disclosed? (Example: Policies, procedures and training are in place so staff know how PI/PHI is to be disclosed. Attach copies of the policies, procedures and training material.) | | | | | | |
| Are there technical safeguards in place to ensure PI/PHI will be used only for authorized purposes? (Example: staff is only given access to parts of databases that contains PI/PHI it needs to complete job duties; documents can be encrypted and/or password protected to ensure only intended recipients can open the documents; audits are completed to ensure staff only accessing PI/PHI it needs for job duties, etc.) | | | | | | |
| Are there physical safeguards in | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| place to ensure PI/PHI is disclosed for authorized purposes? (Example: consideration is given to how records containing PI/PHI is transported or delivered to recipient). | | | | | | |

# PART 2: REMAINING PRIVACY CONSIDERATIONS

## A. RECORDS MANAGEMENT

| Privacy Requirement Questions | Yes | No | Unknown | Explanation | Privacy Impact | Action Items |
|---|---|---|---|---|---|---|
| **RECORDS MANAGEMENT** | | | | | | |
| **RETENTION** | | | | | | |
| Has your organization determined how the PI/PHI being collected, used, and/or disclosed is incorporated into the organization's records management system? | | | | | | |
| Has the medium and format of the PI/PHI been defined? | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| Has the organization determined how long it needs to retain the PI/PHI to be in compliance with applicable legal requirements? | | | | | | |
| **DISPOSITION** | | | | | | |
| Does the organization have procedures to guide the secure disposal of PI/PHI? | | | | | | |
| Will details of the disposal of PI/PHI be recorded? | | | | | | |
| If a third party is retained to dispose of PI/PHI, are contracts or agreements in place to ensure the secure disposal of PI/PHI? Attach copies of the contract or agreements to this PIA. | | | | | | |
| If a third party is retained to dispose of PI/PHI, will the third party issue a certificate of destruction after the PI/PHI has been disposed of? | | | | | | |
| Are there policies or procedures in place that guide employees on how to dispose of PI/PHI? Attach copies of those | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| policies/procedures. | | | | | | |

## B. PRIVACY MANAGEMENT

| Privacy Requirement Questions | Yes | No | Unknown | Explanation | Privacy Impact | Action Items |
|---|---|---|---|---|---|---|
| **ACCOUNTABILITY** | | | | | | |
| What tools are in place to monitor those involved in the management of PI/PHI in carrying out their roles and responsibilities? Explain. (Examples: contracts, agreements, policies, procedures, etc) | | | | | | |
| Is there an employee within your organization that staff can report to if there are questions about the management of PI/PHI? | | | | | | |
| Is there an employee that members of the public can contact if they have questions about the collection, use, disclosure, retention, or disposition of PI/PHI? This employee should be a person who is part of the program area who is leading the project. How is this employee's contact | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| information made known to the public? | | | | | | |
| Is there an employee that members of the public can contact if they want to request correction to their PI/PHI? How is this employee's contact information made known to the public? | | | | | | |
| Is there an employee that members of the public can contact if they want to request access to their PI/PHI? How is this employee's contact information made known to the public? | | | | | | |
| **TRAINING** | | | | | | |
| Is training available to staff so that they understand the policies and procedures are in place to ensure the proper collection, use, disclosure, retention and disposition of PI/PHI? | | | | | | |
| **AUDITING** | | | | | | |
| Will your organization conduct audits to ensure that PI/PHI is being collected, used, disclosed, retained, and disposed of in | | | | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| accordance with the legislation? | | | | | | |
| | | | | | | |