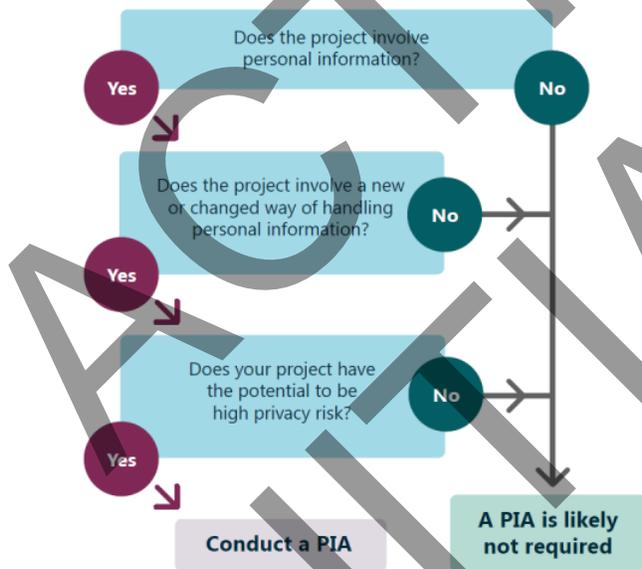


## PIA Determination and Template

PIA#: 22-23

**Here are a few examples of situations where you should consider a PIA:**

- You collect, use or disclose new personal information that you did not collect, use or disclose before.
- You give access to personal information to new parties.
- You implement a new service delivery or management technology that stores, transmits, or retrieves personal information.
- You implement a new or different electronic record system, or make changes to an existing one, such as adding portable devices with wireless network connections.
- You enter into an agreement with a new business partner or vendor who will have access to health information in your custody or control.
- You create a new organization that will collect, use or disclose personal information.



**Please fill out PART A to determine your need for a full PIA.**

## PIA Determination and Template

### PART A

#### 1. Introduction

Answer the who, what, where, when, why and how of your initiative. Describe the initiative in full, including:

##### General Description

###### a) Name of Program or Service:

What is the initiative? **Homewood Health – Employee & Family Assistance Program**

Where will the initiative take place? **For all UNBC Employees and their eligible family members**

Does the work happen online, in person, or both? **Both**

Will there be public events? **Yes, we offer Homewood Health Webinars throughout the year**

Will you hold meetings over the phone, face-to-face, or online? **All of the above. EFAP is a confidential service, so employees meet directly with their counsellors. UNBC is not informed which employees choose to access any EFAP-related services.**

###### b) Name of Department, Branch and Program Area

**Our account executive from Homewood Health is Tracy Brooks.**

###### c) Name of Program or Service Representative:

**Homewood Health has hundreds of registered counsellors across Canada and offer counselling services, life smart coaching and various online resources.**

###### d) Key Program or Service Dates

When will the initiative take place? **Homewood has been providing EFAP services to UNBC employees for many years. We are looking to sign a 2-year contract with a one-year extension.**

Is this a one-time event? **No – see above**

Will the initiative go on for a short time or for the foreseeable future? **See above**

Do you have an end date planned? **End date will depend on signing of contract.**

**PIA Determination and Template**

PIA#: 22-23

**1. Description**

a) Description of the New Program or Service or the Change

t

i. Purposes, Goals and Objectives

To provide confidential, 24/7 access to mental health and wellbeing supports for UNBC employees and their families.

ii. List of All Stakeholders Impacted / Involved

Stakeholder	Role
All UNBC employees	To access EFAP services, if they wish.
Eligible dependents and family members	To access EFAP services, if they wish.
EFAP Counsellors	To provide supportive, confidential and caring counselling supports.

iii. The Need

Why are you doing the initiative? What need does the initiative meet? **To provide confidential, 24/7 access to mental health and wellbeing supports for UNBC employees and their families.**

iv. Governance Model

Accountability – who is ultimately accountable for the program or system? **Director - Human Resources & HR Partner, Employee Health & Wellbeing**

v. Relevant Existing Policies

- None

vi. Related PIAs

- None we're aware of

vii. Relevant contracts

- Previous Homewood Health Contract

viii. Research / Health System Use

Do you anticipate that data collected by this program / system will be used for research or health system use? If so, please explain and provide details of data state (aggregate, de-identified, anonymized etc.)

**No but we do receive quarterly reviews of EFAP usage (anonymous data to identify trends)**

b) The Intended Scope (Project and PIA)

Describe how much of the initiative you will assess in this PIA.

i. Scope of PIA

**PIA Determination and Template**

PIA#: 22-23

- ii. Out of Scope of PIA-this PIA just covers the current contract for Homewood.

**c) Definitions**

Add any applicable definitions here:  
See Appendix C for examples

Term/Acronym	Definition
EFAP	Employee & Family Assistance Program

**2. Personal Information Flow Diagram and Explanation**

If you are collecting, using, storing, sharing, disclosing or retaining Personal Information you will need to proceed with the **Part B and C** of this document.

If not, please sign and send this determination document to the University Governance Office at [privacy@unbc.ca](mailto:privacy@unbc.ca)

Think about the information you'll collect, use, store or share as part of your initiative and list it here. A major part of the PIA process is to make sure that you have authority under the Freedom of Information and Protection of Privacy Act (FOIPPA) to collect, use, store and disclose each of these pieces of information. Limit your collection of personal information to only what is necessary to complete the initiative.

In the table below, complete the Data Element (personal information usually) rationale and method for collection, use, or disclosure highlighting separately by row each instance that information is collected, used, stored, protected, disclosed and disposed of during this initiative.

Unless not possible, ensure these steps are arranged how they would occur chronologically in order to make a transparent workflow. The Privacy Officer will review your steps and determine which type of information management practice each entry is and ensure that the practice is compliant with sections under the Act.

**a) List of Personal health information / personal information / sensitive information to be Collected, Used and/or disclosed and the Rationale for each.**

Please identify each source of data that you intend to access and its business owner. Also indicate that you have contacted the owner and received permission to access the data.

**EXAMPLE:**

**PIA Determination and Template**

PIA#: 22-23

Data Element	Rationale for collection, use or disclosure	Method of Collection or Disclosure
Employee name	To ensure they are an employee	verbal
Employee ID	To ensure they are an employee	verbal

Commented [KH1]: Does Homewood Health document any part of the conversation they have with UNBC employees? If they do, this is personal information.

Note:

Job Category is determined at intake, how does the client identify - which Job Category. Academic Services, CUPE, Exempt, Faculty, Family Member did not use or other. These categories will be listed on the quarterly reporting showing utilization. This information is provided to UNBC on the report but can be optional.

Homewood asks for name and id number when the employee calls them. UNBC does not provide a list of names or employees numbers to Homewood. When Homewood provides UNBC accumulative data they do not provide employee names or numbers (Homewood's operations are based on a trust factor that if the employee is calling and can provide a name and employee number that they will be granted services even though there is no verification process.

Homewood does not disclose the usage of individual services to UNBC or anyone else. They only disclose accumulative usage rates not employee specific usage.

If you do not use personal information in your initiative: how will; you reduce the risk of unintentionally collecting personal information?

For example, if you are collecting opinions as part of a public engagement strategy, participants may offer personal information about themselves or others, even though you've instructed them not to. If you do inadvertently receive or collect personal information, what steps will you take to:

- Destroy it
- Return it
- Transfer it to the correct recipient

FOIPPA section 27.1 describes under what circumstances personal information is considered not collected, despite you having received it. As long as you do nothing with the personal information you receive other than read and delete or return it, or transfer it to the appropriate public body, you have not collected the information according to FOIPPA.

### PIA Determination and Template

**PIA#: 22-23**

However, if you take any other action, including storing the information or using it in your own work, under FOIPPA you have collected personal information without authorization and that is considered a privacy breach.

I am not collecting, using, storing, sharing, disclosing, or deleting any personal information for this initiative.

Staff Name \_\_\_\_\_

Signature \_\_\_\_\_

Date \_\_\_\_\_

**PRIVACY OFFICE USE ONLY**

This initiative does not require a full PIA document.

Privacy Officer name \_\_\_\_\_

Privacy Officer Signature \_\_\_\_\_

Date \_\_\_\_\_

## PIA Determination and Template

PIA#: 22-23

### PART B

#### 3. Collection, Use and Disclosure of Personal Information

Personal Information is being collected under the authority of the University Act and Section 26 of BC's Freedom of Information and Protection of Privacy Act.

##### a) Collection

**Purpose for which personal information may be collected**

26 A public body may collect personal information only if

- (a) the collection of the information is expressly authorized under an Act,
- (c) the information relates directly to and is necessary for a program or activity of the public body,
- (d) with respect to personal information collected for a prescribed purpose,
  - (i) the individual the information is about has consented in the prescribed manner to that collection, and
  - (ii) a reasonable person would consider that collection appropriate in the circumstances,
- (e) the information is necessary for the purposes of planning or evaluating a program or activity of a public body.

**How personal information is to be collected**

27 (1) A public body must collect personal information directly from the individual the information is about unless

- (a) another method of collection is authorized by
  - (i) that individual,
  - (ii) the commissioner under section 42 (1) (i), or
  - (iii) another enactment,

Collection is only permitted through knowledgeable implied or express consent.

##### b) Consent

You may not need a collection notice if:

- You collect personal information indirectly, meaning you get the information from another public body and not from the individual who owns the information
- You collect personal information for law enforcement
- You collect information by observing a person at a public event

FOIPPA section 27(3) and (4) tells you more about when you do not need a collection notice. If you determine that you do not need a collection notice, explain why.

Copy/Paste or Fill in your Privacy/Consent Notice here:

**Use** Please refer to corporate Website Link:

<https://homewoodhealth.com/corporate/privacy-and-records>

**Commented [KH2]:** What happens if this link is broken or changed? Do you have a PDF version. If so, I would suggest you attach it to this PIA as an appendix.

## PIA Determination and Template

PIA#: 22-23

FOIPPA was amended effective November 26, 2021 and those amendments affect this section.

Who will be using the personal information and for what purpose??

Commented [KH3]: Please answer.

### Use of Personal Information

#### Section 32

*A public body may use personal information in its custody or under its control only*

*(a) for the purpose for which that information was obtained or compiled, or for a use consistent with that purpose (see section 34),*

*(b) if the individual the information is about has identified the information and has consented, in the prescribed manner, to the use, or*

*(c) for a purpose for which that information may be disclosed to that public body under sections 33 to 36.*

#### c) Disclosure

To whom will you be disclosing personal information? UNBC does not disclose personal information to Homewood. We will only disclose information as per applicable Canadian privacy laws for access/use/disclosure upon request from the client.

Will it be disclosed to anyone outside of Canada? UNBC does not disclose personal information to Homewood. Homewood No, unless client resides outside of Canada at the time of request for access or disclosure.

Commented [KH4]: I would ask for some clarification around this. Privacy law varies from province to province. I believe HH is based in Ontario.

Commented [KH5]: Since this is a 24 EFAP service, does this mean if a UNBC employee contacts HH after regular business hours, their call is directly connected to someone within Canada? Does

### Disclosure of personal information

*33 A public body may disclose personal information in its custody or under its control only as permitted under section 33.1, 33.2 or 33.3*

#### i. Health System Use

#### ii. Research / Open Data

#### d) The Sources and Accuracy of the Personal Information

It is your responsibility to make sure that the personal information you collect, store, use and disclose is accurate and complete, especially if the information will be used to make a decision that affects an individual. Ways to make sure personal information is accurate and complete include verifying the information with the person it is about prior to recording it.

- Who is providing the information – the individual or another source (e.g. another government department, a family member, provincial program database)? UNBC does not disclose personal information to Homewood.
- Homewood The information is obtained directly from the client
- Is the information as accurate and up to date as is necessary for the purposes for which it would be used and disclosed? UNBC does not disclose personal information to Homewood.

## PIA Determination and Template

PIA#: 22-23

- Homewood states Yes.

FOIPPA section 29 states that a person can ask you to correct any of their personal information in your custody or control. If you cannot correct the record itself, you must make a note on the record (annotate the record). If you've disclosed the personal information to any other public body or third party in the last year, you must also notify them of any corrections you make.

### e) Storage and Location of the Personal Information

FOIPPA was amended effective November 26, 2021 and those amendments affect this section.

#### *Disclosure inside or outside Canada*

33. A public body may disclose personal information referred to in section 33 inside or outside Canada as follows:

in accordance with Part 2;

if the information or disclosure is of a type described in section 22 (4) (e), (f), (h), (i) or (j);

if the individual the information is about has identified the information and consented, in the prescribed manner, to its disclosure inside or outside Canada, as applicable;

Is personal information stored by a service provider?

If you are using a cloud solution, there may be multiple cloud service providers involved in your initiative. Cloud solutions are typically considered to be made up of a 'stack' of infrastructure (IaaS), platform (PaaS) and/or software (SaaS) that might be operated by the same or different cloud service providers. For example, Software as a Service (SaaS) providers often offer services built on infrastructure (IaaS or Infrastructure as a Service) offered by a different cloud service provider.

Provide details on the disclosure, including where and how personal information will be stored. Is the personal information being disclosed outside of Canada?

Homewood - Client information is stored in our on premise Database. This database is encrypted at rest and in transit. It is physically located in Vancouver, back up in Guelph and AWS Toronto. Data is never stored outside of Canada

Describe the contractual terms in place. Here you will describe what type of contract you rely on for your initiative (if applicable). For example, you might be contracting a cloud-based service specifically for your initiative, or you might be using an enterprise offering. Clinician access is restricted to clients that they are currently seeing. At the conclusion of the sessions access for that client information is terminated for that clinician. Clients are identified in the system by birthdate, first name, last name and employer.

What controls are in place to prevent unauthorized access to personal information? Access is not shared with any outside callers and verification questions are asked.

Please provide details on how you will track access to personal information: The CIM department logs all access requests from a client

## PIA Determination and Template

PIA#: 22-23

### Data Linking

N/A

Is the data linking is occurring between either two or more public bodies or one or more public bodies and one or more agencies?

**If this PIA addresses a data-linking program, UNBC must submit this PIA to the Office of the Information and Privacy Commissioner and be subject to their examination, advice and timelines.**

### Common or Integrated Program or Activity

N/A

Please note: If your initiative involves a “data-linking initiative” or a “common or integrated program or activity”, advanced notification and consultation on this PIA must take place with the Office of the Information and Privacy Commissioner (OIPC) as well. Contact the Governance Officer – Access, Privacy and Records Management to determine how to proceed with this notification and consultation in the early stages of developing the initiative, program or activity.

**If this PIA addresses a common or integrated program, UNBC must submit this PIA to the Office of the Information and Privacy Commissioner and be subject to their examination, advice, and timelines.**

#### f) The Retention Schedule and Method of Destruction for Personal Information

##### *Retention of personal information*

##### *31 If an individual's personal information*

*(a) is in the custody or under the control of a public body, and*

*(b) is used by or on behalf of the public body to make a decision that directly affects the individual, the public body must ensure that the personal information is retained for at least one year after being used so that the affected individual has a reasonable opportunity to obtain access to that personal information.*

## PIA Determination and Template

### PIA#: 22-23

Do you use personal information in your initiative to make a decision about an individual? Examples of using personal information to make decisions include but are not limited to:

- Using a person's date of birth or income to decide whether a person qualifies for a benefit
- Using a person's employment history to decide whether they can move forward in a job competition
- Using a person's health information to decide the level and type of care they receive

Keeping information for one year after it is used to make a decision that affects an individual is a minimum requirement under FOIPPA.

You may have other operational or administrative requirements that dictate how long records must be kept and when they must be disposed of. It's important to maintain the records in your initiative according to an approved records schedule.

**Answer here or state N/A:**

If you answered yes above, please describe retention schedules that apply where retention exceeds the one-year requirement under the Act. Please contact the Governance Officer – Privacy, Access and Records Management if you require assistance. Homewood has a data Classification and retention policy.

**Answer here or state N/A:**

### Personal Information Banks

A personal information bank is a collection of personal information that is organized or searchable by the name of the individual or an identifying number, symbol or other identifier. A personal information bank can be a simple list of personal information. Personal information banks contain personal information that is:

- Linked to an identifiable individual
- Organized and capable of being retrieved by a personal identifier
- Normally compiled for a single purpose

Homewood: Client Information is not shared with any outside third-party.

Employer reporting does not contain specific client information and is done only at the aggregate level to ensure privacy.

Briefly describe your personal information bank and the partners and organizations involved.

(N/A)

Name:

Location:

Description:

Authority: This personal information is begin collected under the authority of the University Act and section 26 (a), (c), and (e) of the Freedom of Information and Protection of Privacy Act (FOIPPA).

Purpose:

## PIA Determination and Template

PIA#: 22-23

Category of Users:

Will a database or series of folders be created in this initiative that organizes information by name, identifying number, symbol, or other particular identifier of each individual involved.

If yes, will the records or information collected about the individual contain similar types of personal information. If yes, I will contact the Privacy Officer to ensure that I am identifying that this is a Personal Information Bank (PIB) and identifying the legislatively required descriptors listed in section 69 (6) of FOIPPA.

### g) Method of De-identification/Anonymization/Aggregation for Personal Information

Please explain how Personal Information will be de-identified or anonymized and by whom? Client Information is not shared with any outside third-party.

### h) Users of Personal Information

Please list all users of PI including third parties: Client Information is not shared with any outside third-party.

**Audits :** Please see attachment titled "Audit Logs" for corresponding answers to these questions.

- What does the audit log track? How detailed is the data (e.g., date stamps, time stamps, access control number, IP address, etc.)? Does the audit log include the purpose of an access?
- Are the audit logs immutable?
- Who reads the audit logs, and how long are they kept?
- Who is responsible for oversight of user access?
- Is there a separation of responsibility between those who supervise administration of the system, or security of the system, and those who verify the audit logs (e.g., does the auditor in the organization have a role, or is it the security department?)
- Is the system responsive or passive? For instance, is it possible to put a monitor on particular individuals (e.g., in a hospital setting, if a celebrity is admitted as a patient, etc.)? Will access produce an immediate response and not just a log entry for review months later?
- Will those found to abuse access privileges be sanctioned in a meaningful (and visible) way?

## 4 Access Rights for Individuals to their Personal Information

### Access Request Management

Section 4 of FOIPOP gives individuals the right to access any record under the custody or control of a public body. UNBC is a public body under the Act.

How will you manage access to information requests?

If only aggregate or de-identified data to be released, who is responsible to do so and how is that done?

Homewood: Corporate website link:

<https://homewoodhealth.com/corporate/privacy-and-records>

## PIA Determination and Template

**PIA#: 22-23**

### Request for Personal Information from Persons to Whom It Relates

How will personal requests for access be managed? Personal information is not provided to third party or to family with out clearance or required by law.

**\*\*Please note\*\***

Individuals do not have to make a formal FOI request to access their own personal information held by UNBC.

#### 5 Privacy and Security Safeguards

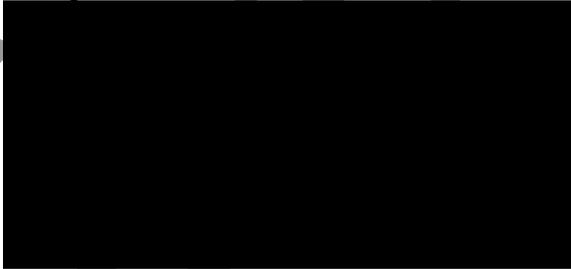
People, organizations and governments outside of your initiative should not be able to access the personal information you collect, use, store or disclose. You need to make sure that the personal information is safely secured in both physical and technical environments.

Does your initiative involve digital tools, databases information systems? IF yes please discuss with ITS whether you also require a security and threat risk assessment

A digital tool, database or information system may leave personal information exposed or otherwise vulnerable to security threats. Security assessments are used on information systems and other digital tools to assess and document security risks, risk ratings and planned risk responses.

#### a) Security Safeguards

- Administrative Safeguards



- Technical Safeguards



## PIA Determination and Template

PIA#: 22-23



- **Physical Safeguards**

This question is to identify how you reduce the risk that you store personal information in a computer system or physical location where unauthorized access can happen.

Technical records are records that are stored electronically, including but not limited to records stored:

- In a database



- On a LAN (local area network)
- On a hard drive
- On a mobile device or laptop

Technical security includes any digital or electronic system set up to keep your records secure, including:

- Using UNBC firewalls
- Encrypting personal information before it is stored or transferred
- Relying on how your cloud service provider protects information in the cloud
- Using passwords to protect digital files and laptops

If your records are not stored on UNBC servers, use this question to list technical security on the system where records are stored.

Physical records include but are not limited to: Homewood states NA

- Paper records
- Film or video
- Photographs
- Audio recordings
- Maps

Physical security is anything you do to keep physical records safe and secure, including:

Homewood has no paper files

- Locking filing cabinets and rooms
- Having security guards that patrol the building
- Restricting access to rooms or buildings where information is stored
- Using alarm systems in the building or room where information is stored

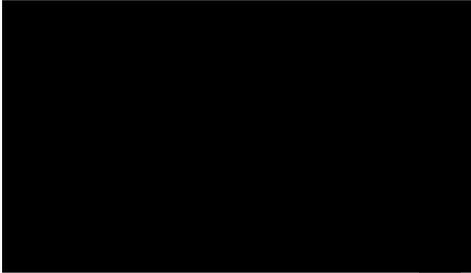
If your physical records are not kept in UNBC buildings with standard UNBC security, use this question to list the physical security in the building and rooms in which records are kept. IF there re not physical records you can skip this section.

Homewood has state N/A



## PIA Determination and Template

PIA#: 22-23



Homewood States not applicable

- Identify any outside partners or companies involved that may have access to the personal information
- Website Domain Ownership (if applicable)

### 6 Privacy Risk Identification and Mitigation

**PIA Determination and Template**

PIA#: 22-23

Risk Rating Overview			
Factor	Risk Rating		
	Low	Medium	High
<b>Nature of personal information</b>	<ul style="list-style-type: none"> <li>✓ Publicly available personal information not associated with any other information</li> </ul>	<ul style="list-style-type: none"> <li>✓ Personal information unique to the organization that is not medical or financial information</li> </ul>	<ul style="list-style-type: none"> <li>✓ Medical, psychological, counselling, or financial information or unique government identification number</li> </ul>
<b>Relationships</b>	<ul style="list-style-type: none"> <li>✓ Accidental disclosure to another professional who reported the breach and confirmed destruction or return of the information</li> </ul>	<ul style="list-style-type: none"> <li>✓ Accidental disclosure to a stranger who reported the breach and confirmed destruction or return of the information</li> </ul>	<ul style="list-style-type: none"> <li>✓ Disclosure to an individual with some relationship to or knowledge of the affected individual(s), particularly disclosures to motivated ex-partners, family members, neighbors or co-workers</li> <li>✓ Theft by stranger</li> </ul>
<b>Cause of breach</b>	<ul style="list-style-type: none"> <li>✓ Technical error that has been resolved</li> </ul>	<ul style="list-style-type: none"> <li>✓ Accidental loss or disclosure</li> </ul>	<ul style="list-style-type: none"> <li>✓ Intentional breach</li> <li>✓ Cause unknown</li> <li>✓ Technical error – if not resolved</li> </ul>
<b>Scope</b>	<ul style="list-style-type: none"> <li>✓ Very few affected individuals</li> </ul>	<ul style="list-style-type: none"> <li>✓ Identified and limited group of affected individuals</li> </ul>	<ul style="list-style-type: none"> <li>✓ Large group or entire scope of group not identified</li> </ul>

Risk Rating Overview			
Factor	Risk Rating		
	Low	Medium	High

**PIA Determination and Template**

PIA#: 22-23

<p><b>Containment efforts</b></p>	<ul style="list-style-type: none"> <li>✓ Data was adequately encrypted</li> <li>✓ Portable storage device was remotely wiped and there is evidence that the device was not accessed prior to wiping</li> <li>✓ Hard copy files or device were recovered almost immediately and all files appear intact and/or unread</li> </ul>	<ul style="list-style-type: none"> <li>✓ Portable storage device was remotely wiped within hours of loss but there is no evidence to confirm that the device was not accessed prior to wiping</li> <li>✓ Hard copy files or device were recovered but sufficient time passed between the loss and recovery that the data could have been accessed</li> </ul>	<ul style="list-style-type: none"> <li>✓ Data was not encrypted</li> <li>✓ Data, files or device have not been recovered</li> <li>✓ Data at risk of further disclosure particularly through mass media or online</li> </ul>
<p><b>Foreseeable harm from the breach</b></p>	<ul style="list-style-type: none"> <li>✓ No foreseeable harm from the breach</li> </ul>	<ul style="list-style-type: none"> <li>✓ Loss of business or employment opportunities</li> <li>✓ Hurt, humiliation, damage to reputation or relationships</li> <li>✓ Social/relational harm</li> <li>✓ Loss of trust in the public body</li> <li>✓ Loss of public body assets</li> <li>✓ Loss of public body contracts or business</li> <li>✓ Financial exposure to public body including class action lawsuits</li> </ul>	<ul style="list-style-type: none"> <li>✓ Security risk (e.g. physical safety)</li> <li>✓ Identify theft or fraud risk</li> <li>✓ Hurt, humiliation, damage to reputation may also be a high risk depending on the circumstances</li> <li>✓ Risk to public health or safety</li> </ul>

Please identify any privacy risks, even very unlikely ones, associated with the initiative and the mitigation strategies that will be implemented. Please provide details of all such strategies. The Privacy Officer will help identify the likelihood (low, medium, or high) of this risk happening and the degree of impact it would have on individuals if it occurred.

Please explain the risks in detail using the associated CSA Model Code (Appendix B).

**EXAMPLE**

**PIA Determination and Template**

**PIA#: 22-23**

<p><b>Risk # 1</b></p> <p>Data that is no longer needed is at risk of being breached because it is being retained in the IT platform longer than necessary.</p> <p><b>Related CSA Principle:</b></p> <p><b>Safeguards</b></p>	<p><b>Cause:</b> Data is not being deleted from the IT platform in a timely manner once it is no longer needed.</p>
	<p><b>Probability:</b></p> <p>Low</p>
	<p><b>Impact:</b></p> <p>High</p>
	<p><b>Mitigation:</b></p> <p>Implement a process on the IT platform that automatically deletes data once it is no longer needed, per the policy established by X</p>

<p><b>Risk # 1</b></p> <p><b>Related CSA Principle:</b></p>	<p><b>Cause:</b></p>
	<p><b>Probability:</b></p>
	<p><b>Impact:</b></p>
	<p><b>Mitigation:</b></p>

<p><b>Risk # 2</b></p> <p><b>Related CSA Principle:</b></p>	<p><b>Cause:</b></p>
	<p><b>Probability:</b></p>
	<p><b>Impact:</b></p>

**PIA Determination and Template**

PIA#: 22-23

	<b>Mitigation:</b>
--	--------------------

<b>Risk # 3</b>  <b>Related CSA Principle:</b>	<b>Cause:</b>
	<b>Probability:</b>
	<b>Impact:</b>
	<b>Mitigation:</b>

**PART C**

**Conclusions and Approvals**

Once the PIA has been approved with or without conditions, the Privacy Officer will collect signatures from the individuals provided below. A copy of the PIA will be distributed to all signatories for convenience or to attach to a requisition or file with a contract.

**Name of Individual leading the Program/Project:** \_\_\_\_\_

I confirm the information management practices in this initiative have been documented on Form A, and B as applicable, as accurately as I am aware and I commit to communicating appropriate information management practices to all individuals participating in this initiative as appropriate. I commit to following the documented practices on this PIA, or arranging a PIA amendment if I am aware information management practices in this initiative change.

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

**Director or Dean Overseeing the Program/Project:**  Kerry Roberts

I am accountable for overseeing my staff involved in this initiative to ensure they adhere to information management practices presented in this PIA. I will arrange for the project lead named above to contact the Privacy Officer to arrange a PIA amendment if required.

Signature:  Kerry Roberts  Date:  November 03, 2022

**PIA Determination and Template**

**PIA#: 22-23**

**Chief Information Security Officer**

Signature: \_\_\_\_\_ Dave Kubert \_\_\_\_\_ [Redacted] \_\_\_\_\_ Date: \_\_\_\_\_ Nov. 14, 2022 \_\_\_\_\_

Note: The security assessment for the service provider is satisfactory and the CISO signature attests to that. However, there have been no risks or mitigations identified in this PIA. It is highly unlikely that there are no risks to privacy associated with this project.

**Privacy Officer:** \_\_\_\_\_

I confirm that this initiative to the best of my knowledge as written in Form A, and B as applicable, has information management practices that comply with British Columbia's Freedom of Information and Protection of Privacy Act.

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

ACTIVELY INITIATIVE

## PIA Determination and Template

PIA#: 22-23

### APPENDIX 1 DEFINITIONS

---

**Confidentiality**

The assurance that information about identifiable persons, the release of which would constitute a privacy breach, will not be disclosed without consent, except as allowed by law.

---

**Consent**

Consent, in the context of personal information, means the agreement of someone to provide their personal information for the purposes identified to them. In some cases, consent may not be possible (e.g., medical emergency) or may not be required (e.g., collection by police of information relating to a suspect where the collection is not a search or seizure). Consent is generally given by a specific act of the individual, but sometimes it can be implied. In the public sector, consent is not always a requirement for the collection of personal information – having the legal authority to collect personal information is.

---

**Core privacy principles**

In March 1996, the Canadian Standards Association (CSA) developed a national, voluntary code that sets basic principles for safeguarding personal data. The Code establishes 10 basic principles for all organizations that collect or use personal information. In some cases, certain principles may not apply to public sector regimes. For example, in the public sector, the “consent” principle listed as number three below is often substituted for “legal authority”.

1. *Accountability* - An organization is responsible for personal information under its control and shall designate an individual or individuals who are accountable for the organization's compliance with the following principles.
  2. *Identifying Purposes* - The purposes for which personal information is collected shall be identified by the organization at or before the time the information is collected.
  3. *Consent* - The knowledge and consent of the individual are required for the collection, use or disclosure of personal information, except where inappropriate.
-

**PIA Determination and Template**

**PIA#: 22-23**

4. *Limiting Collection* - The collection of personal information shall be limited to that which is necessary for the purposes identified by the organization. Information shall be collected by fair and lawful means.
5. *Limiting Use, Disclosure and Retention* - Personal information shall not be used or disclosed for purposes other than those for which it is collected, except with the consent of the individual or as required by law. Personal information shall be retained only as long as necessary for the fulfillment of the stated purposes.
6. *Accuracy* - Personal information shall be as accurate, complete and up-to-date as is necessary for the purpose for which it is used.
7. *Safeguards* - Personal information shall be protected by security safeguards appropriate to the sensitivity of the information.
8. *Openness* - An organization shall make specific information about its policies and practices relating to the management of personal information readily available to individuals.
9. *Individual Access* - Upon request, an individual shall be informed of the existence, use, and disclosure of his or her personal information, and shall be given access to that information. An individual shall be able to challenge the accuracy and completeness of the information and have it amended as appropriate.
10. *Challenging Compliance* - An individual shall be able to address a challenge concerning compliance with the above principles to the designated individual or individuals accountable for the organization's compliance.

**Data (information) flows** Mapping the flow and manipulation of information within and across systems or business processes.

**Data matching** An activity that involves comparing personal data obtained from a variety of sources, including personal information banks, for the purpose of making decisions about the individuals to whom the data pertains. Included in this definition of data-matching is data linkage, also known as data profiling.

**Personal information** For data to be categorized as *personal* information (rather than just information, in general), it must have details sufficient to identify an individual. Individual identification is thus the threshold for transforming general information into personal information and where rights, protections, and requirements associated with the proper handling of personal information are triggered.

Without restricting the generality of the foregoing, personal information may include, for example:

## PIA Determination and Template

PIA#: 22-23

---

- information relating to the race, national or ethnic origin, colour, religion, age or marital status of the individual,
- information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,
- any identifying number, symbol or other particular assigned to the individual,
- the address, fingerprints or blood type of the individual.
- the personal opinions or views of the individual except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual by a government institution or a part of a government institution specified in the regulations.
- correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence.
- the views or opinions of another individual about the individual.
- the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual by an institution or a part of an institution referred to in paragraph (e), but excluding the name of the other individual where it appears with the views or opinions of the other individual, and,
- the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual,

In some jurisdictions, personal information **may not include** information about an individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual including,

- the fact that the individual is or was an officer or employee of the government institution,
  - the title, business address and telephone number of the individual,
  - the classification, salary range and responsibilities of the position held by the individual
  - the name of the individual on a document prepared by the individual in the course of employment, and,
  - the personal opinions or views of the individual given in the course of employment.
  - information about an individual who is or was performing services under contract for a government institution that relates to the services performed, including the terms of the contract, the name of the individual and the opinions or views of the individual given in the course of the performance of those services,
-

**PIA Determination and Template**

**PIA#: 22-23**

- information relating to any discretionary benefit of a financial nature, including the granting of a license or permit, conferred on an individual, including the name of the individual and the exact nature of the benefit, and
- information about an individual deceased for more than twenty years.

**Privacy**

Privacy is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others.

**Privacy officer**

A privacy officer is a person within an organization whose job it is to:

- encourage compliance with sound privacy principles, prevailing privacy policies and privacy laws;
- respond to requests for access to and correction of personal information and general issues within a public body concerning personal information; and
- work with information and privacy commissioners during the investigation of a privacy complaint against an organization.

Privacy officers may also be responsible for managing changes to an organization's:

- information management practices, policies and procedures;
- staff training, vis-a-vis privacy and information handling;
- privacy policies and procedures; and
- inquiry and complaint processes.

**Privacy protection**

Preventing unauthorized collection, use and disclosure of an individual's personal information.

**Program manager**

The person responsible for managing and directing the projects of a public body, with emphasis on coordinating and prioritizing resources, and managing the risks which emanate from projects in development or underway. Program managers are responsible for ensuring that the projects they lead or direct are compliant with government policies and the law.

**Risk assessment**

The process of quantifying the impact of implementing a particular idea, process, system or strategy.

**Threat and Risk Assessment (TRA)**

A risk management process used to evaluate the security threats associated with information technology projects, including potential system vulnerabilities and impacts on data integrity and confidentiality. TRAs, when completed in

**PIA Determination and Template**

**PIA#: 22-23**

---

conjunction with a PIA, can help provide recommendations to lower information and privacy risks to acceptable levels.

---

ACTIVE INITIATIVE

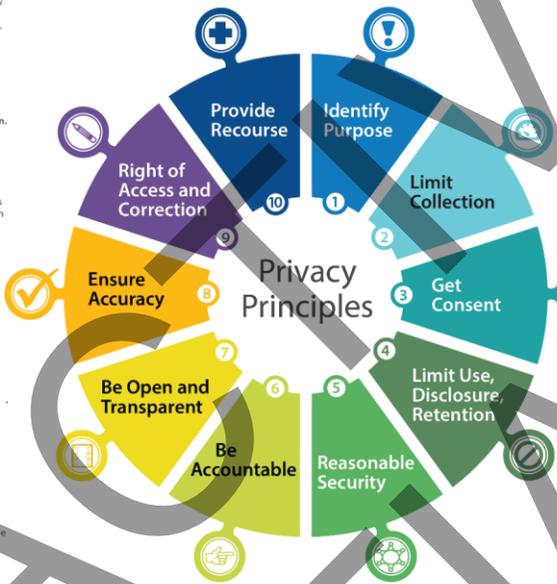
## PIA Determination and Template

PIA#: 22-23

### APPENDIX B CSA MODEL CODES

#### The 10 Privacy Principles

10. **Provide Recourse.** If you receive a complaint about how an individual's personal information has been handled, direct it to the Privacy, Compliance and Training Branch immediately, via the breach reporting line: 7-7000, option 3. Learn more from link provided below.
9. **Right of Access and Correction.** Individuals have a right to access their own personal information, or have that information corrected. Be aware of the FOI process, and direct any requests to Information Access Operations immediately. More information provided at link below.
8. **Ensure Accuracy.** You must make a reasonable effort to ensure personal information collected is accurate and complete if it will be used to make a decision affecting the individual it is about. Find out more about this requirement at the link below.
7. **Be Open and Transparent.** Routinely release any records that can be regularly provided to the public. Proactively disclose any records that will be of interest to the public. Consult with Information Access Operations on these processes. Find the Open Information Open Data Policy provided at the link below.
6. **Be Accountable.** Be responsible for all personal information under your control, including contractors' records. Be aware of who your Ministry Privacy Officer is. Find your MPO at the link below.



1. **Identify Purpose.** Must identify in writing: the purpose for which you are collecting personal information, the legal authority and contact information of someone who can answer questions about the collection, unless an exception applies. See link below for more.
2. **Limit Collection.** Do not collect personal information indiscriminately or without a legal authority. Information must be necessary to fulfill identified purposes, and be reasonable and appropriate. Find more information at the link below.
3. **Get Consent.** Secure consent as a means to **access** or disclose personal information for secondary purposes. Consent must be **affirm** and explicit. There are some specific circumstances where consent is not required. See the link below.
4. **Limit Use, Disclosure, Retention.** You may use or disclose personal information for the purposes identified when it was collected, or another reason authorized by FOIPPA. For new uses, get consent. More information provided at the link below.  
**Limit Retention.** Personal information used to make a decision about an individual must be retained for at least one year. Information must be destroyed in accordance with any applicable records retention schedules. Find your Records Officer at the link below.
5. **Reasonable Security.** Must make reasonable security arrangements to protect personal information. Measures should be appropriate and proportional to the sensitivity of the information. Consideration should be given to physical, technical and procedural measures. Find your MISO at the link below.

For more information on the privacy principles and resources, visit: [www.gov.bc.ca/privacyprinciples](http://www.gov.bc.ca/privacyprinciples)

## PIA Determination and Template

PIA#: 22-23

### APPENDIX C

#### SAMPLE PRIVACY AND CONSENT NOTICE

##### WE NEED TO COLLECT INFORMATION FROM YOU

UNBC Continuing Studies needs to collect information from you to:

1. Enroll you
2. Confirm sponsorship arrangements
3. Process your payment
4. Generate a class list for instructors
5. Ensure that grades and certificates are assigned to the correct student
6. Assist our partners in verifying certificate validity

##### WE HAVE PERMISSION TO DO THIS

The University of Northern British Columbia collects, uses, shares, discloses, maintains and when applicable deletes and destroys Personal Information provided on this form according to the *Freedom of Information and Protection of Privacy Act* [RSBC 1996 c. 165].

##### HOW WE WILL USE AND SHARE YOUR INFORMATION

Continuing Studies must directly disclose some information on this form and your course completion status to your sponsor, including your employer if you are sponsored through your job. Continuing Studies may need to share the information on this form with anyone repairing or maintaining electronic systems involved in this Continuing Studies course.

UNBC Continuing Studies is the training agency chosen to deliver the Wildlife Dangerous Tree Assessor courses on behalf of the Wildlife Dangerous Tree Committee of BC (WDTC). Under the terms of our agreement with the WDTC, Continuing Studies provides a list of current assessors upon request. Under the terms of this agreement UNBC also provides a list of current Fire assessors to BC Wildfire Services (BCWS), twice a year to support certificate verification. Personal information on this form will be shared confidentially with members of the WDTC. Certificate status, certificate number and copies of certificates may be shared upon request by contractors and employers for the purpose of confirming qualifications. You have the right to revoke consent to the collection, use, retention, and disclosure of personal information at any time, but doing so will result in consequences including, but not limited to, forfeiting registration in the course.

##### HOW WE WILL PROTECT YOUR INFORMATION

UNBC is obligated to protect your personal information and has various processes in place to ensure it is secure.

##### HOW LONG WE WILL KEEP YOUR INFORMATION

The *Freedom of Information and Protection of Privacy Act* allows us to keep your Personal Information for at least one year after collection and when its period of usefulness is over we will securely delete or destroy it. In the case of the Wildlife Dangerous Tree Assessor Certificate Program, hardcopy materials are kept for the life of the Certificate, which is four years, before being destroyed.

##### WHAT TO DO IF THE INFORMATION WE HAVE COLLECTED FROM YOU IS INCORRECT, OR YOU HAVE QUESTIONS?

### PIA Determination and Template

**PIA#: 22-23**

Please contact UNBC Continuing Studies at: 250-960-5980 OR [cstudies@unbc.ca](mailto:cstudies@unbc.ca)

If you still have questions or concerns, please contact: Doris Marshall-Greenlaw, Governance Officer for Access, Privacy and Records Management at 250-960-5139 OR [privacy@unbc.ca](mailto:privacy@unbc.ca)

By registering for this course, you indicate you have read, understand, and agree to the privacy statement. You also understand that you have the option to ask questions about any part of this statement before registering.

Signature: \_\_\_\_\_ Date: \_\_\_\_\_

ACTIVELY INITIATIVE