UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

Privacy Impact Assessment

Oracle Hyperion

Form adapted from the BC Government template for Non-Ministry Public Bodies. June 2014

PIA# *18-017* *(Office of the University Secretariat to assign)*

Why do I need to do a PIA (Privacy Impact Assessment)?
Section 69(5.3) of the *Freedom of Information and Protection of Privacy Act* (FIPPA) requires the head of a public body to conduct a privacy impact assessment (PIA) in accordance with the directions of the minister responsible for FIPPA. Public bodies should contact the Information Governance Officer to determine internal policies for review and sign-off of the PIA. If you have any questions about this PIA template or FIPPA generally, please contact Adam Cullum (Information Governance Officer) at adam.cullum@unbc.ca or (250) 960-5139 or visit http://www.unbc.ca/foippa.

What if my initiative does not include personal information?
Public bodies still need to complete Part 1 of the PIA and submit it along with the signatures pages to Information Governance Officer even if it is thought that no personal information is involved. This ensures that the initiative has been accurately assessed.

Part 1 – General

Name of Department:	University Integrated Planning		
PIA Drafter:	Sheena Smith		
Email:	Sheena.Smith@unbc.ca	Phone:	**250 960 5106**
Department Manager:	**Bernadette Patenaude**		
Email:	Bernadette.Patenaude@unbc.ca	Phone:	**250 960 5334**

In the following questions, delete the descriptive text and replace it with your own.

1. Description of the Initiative

Oracle Hyperion is a cloud-based service to manage, model and customize how we plan university budgets and track revenues and expenditures. Primary functions of the software include strategic financial forecast models, financial framework and statement models, workforce compensation and planning models, project management frameworks, and capital planning frameworks.

2. Scope of this PIA

Determined by Specifications when available.

3. Related Privacy Impact Assessments

This section will identify if any other PIAs have been completed or are in the processes of being conducted that are related to this PIA. The Information Governance Officer may need to complete this question.

4. All Elements of Information or Data

- *GL, and other budget and forecasting data*
- *Salary types*
- *Tuition*
- *Grand Revenue*
- *Budget Aggregation*

If personal information is involved in your initiative, please continue to the next page to complete your PIA.

If no personal information is involved, please submit Parts 1, 6, and 7 to the Information Governance Officer for review. You will receive support completing the remaining steps of the PIA.

Part 2 – Protection of Personal Information

In the following questions, delete the descriptive text and replace it with your own.

5. Storage or Access outside Canada

Please provide a brief description of whether your information can be accessed from outside Canada, for example, by a service provider that is repairing a system, or if your information is being stored outside Canada, for example, in the "cloud". If your data is stored within Canada and accessible only within Canada, please indicate this. The Information Governance Officer or CIO will require proof that you have investigated and understand where active and backup records are stored.

6. Data-linking Initiative*

In FIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act. If you answer "yes" to all 3 questions, your initiative may be a data linking initiative and you must comply with specific requirements under the Act related to data-linking initiatives.	
1. Personal information from one database is linked or combined with personal information from another database;	yes/no
2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	yes/no
3. The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	yes/no
If you have answered "yes" to all three questions, please contact the Information Governance Officer to discuss the requirements of a data-linking initiative.	

7. Common or Integrated Program or Activity*

In FIPPA, "common or integrated program or activity" is strictly defined. Answer the following questions to determine whether your initiative qualifies as "a common or integrated program or activity" under the Act. If you answer "yes" to all 3 of these questions, you must comply with requirements under the Act for common or integrated programs and activities.	
1. This initiative involves a program or activity that provides a service (or services);	yes/no
2. Those services are provided through: (a) a public body and at least one other public body or agency working collaboratively to provide that service; or (b) one public body working on behalf of one or more other public bodies or agencies;	yes/no
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	yes/no
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	

**** 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 Information Governance Officer to determine how to proceed with this notification and consultation in the early stages of developing the initiative, program or activity.***

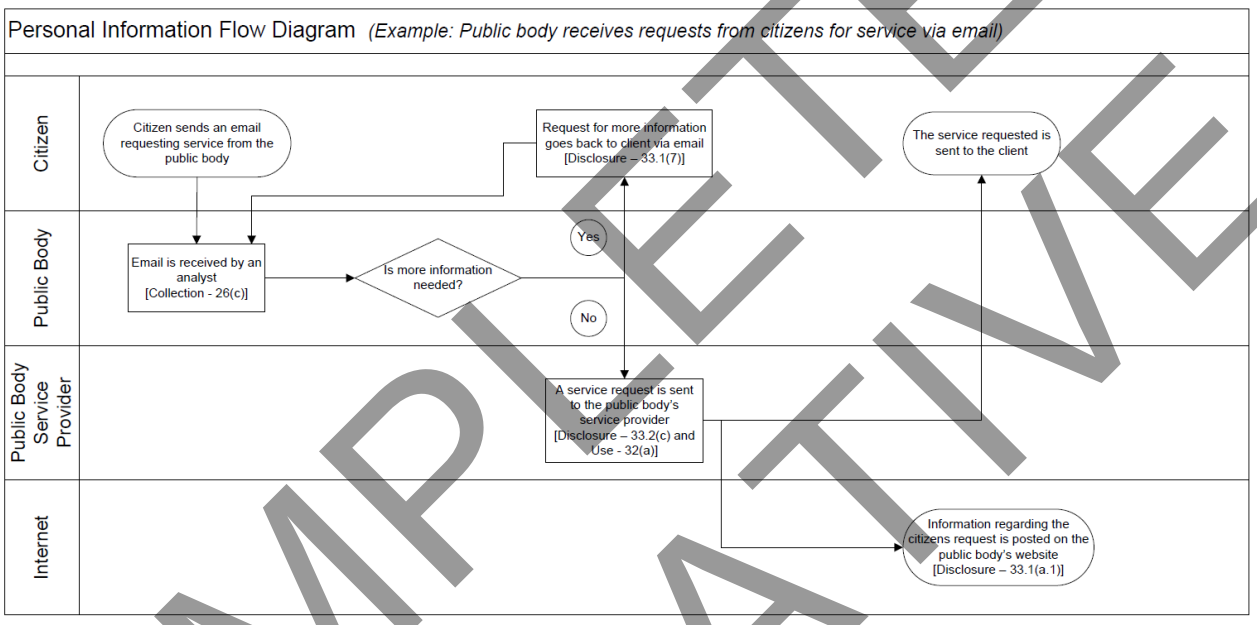
8. Personal Information Flow Diagram and/or Personal Information Flow Table

Please provide a diagram and/or table that shows how your initiative, program or IT solution will collect, use, and/or disclose personal information (see examples below). Your diagram and/or table must also include the authorities for the collection, use, and disclosure of personal information, as laid out in FIPPA. It should also outline the flows of personal information wherever it is transmitted or exchanged. ***Both a flow diagram and a table must be included if the PIA is related to a common or integrated program or activity or a data-linking initiative.***

For ease of reference, the collection, use, and disclosure authorities in FIPPA can be found in the appendices. If you do not know what the relevant authorities are, please contact the Information Governance Officer.

Depending on the complexity of your initiative, you may choose to provide one general diagram for the initiative, and more specific diagrams for particular components. If multiple organizations will collect, use, or disclose personal information, the diagram should identify how each organization is involved in the initiative.

Example:



Remove examples and replace them with how personal information flows in your initiative under Description/Purpose. Separate each step into a new row and place these steps in chronological order of how the information is used. Add additional lines as needed until you have completely described all collection, use, disclosure, and disposition of the information. The Information Governance Officer will complete the type and FIPPA authority columns.

Personal Information Flow Table

	Description/Purpose	Type	FIPPA Authority
1.	*Email received from client requesting service*	*Collection*	*26(c)*
2.	*Email client back requesting more information*	*Disclosure*	*33.1(7)*
3.	*Service request transferred to service provider contracted by public body*	*Disclosure & Use*	*33.2(c) and 32(a)*

9. Risk Mitigation Table

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. Also,

please identify the likelihood (low, medium, or high) of this risk happening and the degree of impact it would have on individuals if it occurred.

Examples can be removed and additional lines added as needed.

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	[redacted]			
2.				
3.				
4.				

10. Collection Notice

If your initiative is collecting personal information directly from individuals you must ensure that all individuals involved are told the following:

1. *The purpose for which the information is being collected*
2. *The legal authority for collecting it, and*
3. *The title, business address and business telephone number of an officer or employee who can answer questions about the collection.*

Please include your proposed wording for a collection & consent notice and where it will be located for individuals to read before collection takes place. You can also attach a screen shot or a copy of your form where the collection notice would be located.

Part 3 – Security of Personal Information

Please consult with the Information Governance Officer, the Chief Information Officer or the IT Security Officer when filling out this section if you have any questions.

11. **Please describe the physical security measures related to the initiative (if applicable).**

For example: locked cabinets, securely stored laptops, or key card access to the building.

12. Please describe the technical security measures related to the initiative (if applicable).

For example: use of firewalls, document encryption, or user access profiles assigned on a need-to-know basis.

13. Does your department rely on any security policies? If so, indicate here:

Please describe any specific policies and procedures and provide contact details for someone who could answer further questions regarding these policies and procedures.

14. Please describe any access controls and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

For example: role-based access.

15. Please describe how you track who has access to the personal information.

For example: audit trails or physical sign-in and sign-out of files.

Part 4 – Accuracy/Correction/Retention of Personal Information

16. How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated. If personal information will be disclosed to others, how will the public body notify them of the update, correction or annotation?

For example: users have access to update their own information or, notes will be made on a case file.

17. Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.

18. If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

For example: check to see that the information was obtained from a reputable source.

19. If you answered "yes" to question 17, do you have a records retention and/or disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?

If you do not yet have a schedule, please document how these records will be kept until the schedule is in place. Please describe retention schedules that apply where retention exceeds the one year requirement of FIPPA. Please contact the Information Governance Officer if you require assistance.

Part 5 – Further Information

20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

For example: your department has a regular exchange of personal information (both collection and disclosure) to provide services to your clients.

Please check this box if the related Information Sharing Agreement (ISA) is attached. If you require assistance completing an ISA, please contact the Information Governance Officer.	

21. Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

For example: your public body will be disclosing information to PhD students so that they can conduct research.

Please check this box if the related Research Agreement (RA) is attached. If you require assistance completing an RA please contact the Information Governance Officer, the UNBC Research Office or UNBC Archives.	

22. Will a personal information bank (PIB) result from this initiative? If yes, please list the legislatively required descriptors listed in section 69 (6) of FIPPA. Under this same section, this information is required to be published in a public directory.

A personal information bank means a collection of personal information that is organized or retrievable by the name of an individual or by an identifying number, symbol, or other particular assigned to an individual.

Please ensure Parts 6 and 7 are attached to your submitted PIA.

Part 6 – Comments, Conditions & Concerns

This PIA is based on a review of the material provided to the Information Governance Officer as of the date below. If, in future any substantive changes are made to the scope of this PIA, the public body will have to complete a PIA update and submit for approval.

Part 7 – Program Area Signatures

Name of Individual leading the Program/Project *(Normally the individual who completed the PIA)*	Signature	Date
Department Head	Signature	Date
Director or Dean Overseeing the Program/Project	Signature	Date
Contact Responsible for Systems Maintenance and/or Security *(if applicable)*	Signature	Date
Information Governance Officer (Privacy Officer)	Signature	Date
Head of Public Body or Designate	Signature	Date

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

A final copy of this PIA (with all signatures) will be kept on record with the Information Governance Officer.