UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

Privacy Impact Assessment Form

PIA # and Name- # 22-045 MOIS

1 Key concepts

Contents

ACTIVE INITIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

ACTIVE INITIATIVE

“personal information” means recorded information about an identifiable individual, including,

(a) information relating to the race, national or ethnic origin, colour, religion, age, sex, sexual orientation or marital or family status of the individual,

(b) information relating to the education or the medical, psychiatric, psychological, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

(c) any identifying number, symbol or other particular assigned to the individual,

(d) the address, telephone number, fingerprints or blood type of the individual,

(e) the personal opinions or views of the individual except where they relate to another individual,

(f) correspondence sent to an institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to that correspondence that would reveal the contents of the original correspondence,

(g) the views or opinions of another individual about the individual, and

(h) the individual’s name where it appears with other personal information relating to the individual or where the disclosure of the name would reveal other personal information about the individual.

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

2 General Information

1. Name of Department, Branch and Program Area

Under the Student Success portfolio this software is being used by UNBC's student Medical Clinic as well as Student Counsellor centre

2. Name of Program or Service Representative

Overall day-to-day use of the software is overseen by the Manager of Wellness (managing services & staff within the Medical Clinic, Counselling Centre and the Access Resource Centre - ARC);Manager reports directly to the Director of Student Success

3. When will the initiative take place? 2/18/23

4. Is this a one-time event?

☐ Yes ☑ No

5. Do you have an end date planned?

☐ Yes ☑ No

6. Describe the New Program or Service or the Change

Moving the current MOIS software and associated data to a cloud based service that is overseen by the vendor of the software Bright Health

ACTIVE INITIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

7. Describe the Purposes, Goals and Objectives

Why are you doing the initiative? What need does the initiative meet?

The purpose of this move is twofold:
1) Provide the most up-to-date MOIS toolset to the UNBC users of the product;

2) Gain internal IT resource efficiencies both from a staff as well as a financial (operating as well as capital) perspective. This Cloud services places the responsibility for software maintenance on the vendor vs the vendor pushing out updates that we would have to apply. Using a Azure based cloud service the vendor has access to network resources that we could not easily match internally therefore backup of data and service up time is increased. The software as a service in the cloud maintains the same look and feel as if it remained internal with small changes in workflow re scanning.

8. Describe the Governance Model

Accountability – who is ultimately accountable for the program or system

The Manager of Health and Wellness is responsible to oversee UNBC's users access and use of the system and overall data entry practices. The Manager of Health and Wellness reports to the Director of Student Success who ensures that the Manager has developed appropriate policies and audit practices around this system and its data.The Director is also responsible to approve all new users to the system.

ACTIVE INITIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

9. List of All Stakeholders Impacted / Involved

Stakeholder	Role
Students	All students who use the Medical Clinic or Counselling Services will have personal information stored in this system.
5 Counsellors and 1 Counselling Coordinator	All counsellors will use this system from intake through completion of service. Look and feel of system will be the
1 Counselling Student Services Representative -	Student Services Representative will continue to use the cloud based system with no change in functionality. One
Up to two practicum students during Fall and	As new users to the system they will be orientated to the system and there shouldn't be any issue with the cloud based
2 Nurse Coordinators (Job share at .51 FTE	Nurse Coordinators will continue to use the cloud based system with no change in functionality. Logging into the
Under agreement with Northern Health - clinic is	If these Primary Health Care providers use UNBC computers they will be provided with logins for the computers and will
1 Health Services Assistant - front	Health Services Assistant will continue to use the cloud based system with no change in functionality. One specific
1 Manager of Health & Wellness	Manager will continue to use the cloud based system with no change in functionality. Logging into the system will be
Faculty	No change - they do not have access to the system and are not provided specific information on a students health or

10. Please add any additional comments below.

IT is also impacted to ensure the Cloud Service interacts effectively within our internal network and they support on premise technical issues with scanning and printing that can not be dealt with by the vendor.

11. Describe any Relevant Existing Policies

At the time of this PIA the only active policy that has impact in this area is the policy covering Confidentiality of Student Records

ACTIVE INITIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

12. Describe any Related PIAs

NA

13. Describe any Relevant contracts

Bright Health has a End User License Agreement (EULA) that covers the contractual obligations of using this software.

There is an existing contract with NH to ensure their Primary Care Providers are able to access our instance of MOIS

14. Research / Health System Use

Do you anticipate that data collected by this program / system will be used for research or health system use?

☐ Yes ☑ No

15. If so, please explain and provide details of data state (aggregate, de-identified, anonymized etc.)

3 Collection, Use, and Disclosure

16. What are the data or information elements involved in your initiative?

Please list all the elements of information or data that you might collect, use, store, disclose, or access as part of your initiative. If your initiative involves large quantities of information or datasets, you can list categories or other groupings of personal information in a table below or in an appendix

ACTIVE INITIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

FIPPA Section	Authority to Collect Personal Information
26(a)	The collection of the information is expressly authorized under an Act
26(b)	The information is collected for the purposes of law enforcement
26(c)	The information relates directly to and is necessary for a program or activity of UBC
26(e)	The information is necessary for the purposes of planning or evaluating a program or activity of UBC
26(f)	The information is necessary for the purpose of reducing the risk that an individual will be a victim of domestic violence, if domestic violence is reasonably likely to occur
26(g)	The information is collected by observation at a presentation, ceremony, performance, sports meet or similar event at which the individual voluntarily appears, and that is open to the public

Data Element	Rationale for collection, use or disclosure	Method of Collection or Disclosure	FIPPA Section
Demographic data	Standard information to allow clinic/counsellor staff with information on	Completed form entered	26(c)
Clinic health history intake	Provides a summary of medical history and lifestyle choices	Completed form	26(c)
Counselling walk in form	To provide direction for the session and the goals as well as clarify best support	paper form and scanned	26(c)
Clinic/Counselling/ARC	Disclosure to student users of services re sharing of information; FOI sections;	Completed form	26(c)
Session notes/Encounte	Continuance of overall health care	Electronic notes within	26(c)
Requests for additional	Continuance of overall health care	In person sessions with	26(c)
Pharmanet Consent form	Provincial Initiative to confirm all prescriptions provided to a person in BC	Completed form signed	26(c)

ACTIVE INITIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

3.1 Collection Notice

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. personal information may be collected only if such collection is authorized by or under legislation, essential for operating programs or activities, or collected for law enforcement purposes.

If you are collecting personal information directly from the individual the information is about, FOIPPA requires that you provide a collection notice (except in limited circumstances).

17. Describe how personal information is to be collected

All users complete a Client Intake form and a Consent form prior to the start of any clinic or wellness service. Each session with the client, notes are recorded within MOIS so that in subsequent appointments continuum of care can be provided

18. Review the sample collection notice and attach the notice as an appendix.

(See Appendix C for an example)

ACTIVE INITIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

3.2 Use

19. Please list all users of PI including third parties

Counsellors
Practicum Student
Counselling Coordinator
Counselling Service Representative

Nurse Coordinator
Health Services Assistant

Northern Health (NP and Physician)

Manager Health & Wellness

20. Describe how personal information is to be used

All the information collected is to support a heath/care plan for the student accessing the service. We also collect individuals Personal Health Number (PHN) that is required for billing purposes; emergency contact info is collected and used in case of medical emergency.

3.3 Disclosure

Section 26 states that 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. A public body may

ACTIVE INITIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

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.

21. To whom will you be disclosing personal information?

Provide details on the disclosure, including where and how personal information will be stored.

Following the shared care model, information related to specific students will be provided to other health professionals to support the health care plan agreed to with the student.

If a student requests that their file be shared with another health professional we will obtain their consent on this and we will forward. This may include students from outside of Canada (International Students) and at their request we will forward records to their local/international health provider.

No disclosure of personal information will occur without consent from the student unless
- Possibility of child at risk of abuse or neglect;
- Imminent risk that a student will harm oneself or others
- A Court of Law or the Ministry of Children & Family Development lawfully demands the information

ACTIVE INITIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

22. Will it be disclosed to anyone outside of Canada?

Provide details on the disclosure, including where and how personal information will be stored.

The only disclosure outside of Canada would be at the request of the student to do so and it would usually be related to International Students who request their wellness records sent to a health provider where they are returning to after graduation.

23. Will it be disclosed as part of Health System Use?

Provide details on the disclosure, including where and how personal information will be stored.

No personal information will be disclosed for overall Health System use. We will provide usage patterns of our services and aggregated numbers in support of overall demand for resources and potentially for increases of resources in a certain areas.

24. Will it be disclosed as part of Research / Open Data?

Provide details on the disclosure, including where and how personal information will be stored.

NO

ACTIVE INITIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

4 Storage and Location of the Personal Information

25. Is any personal information stored outside of Canada?

☐ Yes ☑ No

26. Describe how PI information will be stored

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.

[redacted]

The MOIS offering in the cloud would be characterized as SaaS hosted in Microsoft Azure (IaS/PaS)

ACTIVE INITIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

27. 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.

Cloud based service that support health & wellness activities associated with UNBC's Student Medical Clinic and Student Counselling Services by provided an electronic medical record (EMR) system.

Contractually we pay for this services based on the number/type of users we have active in the system plus a fee for cloud hosting as well as a fee for multi factor authentication (MFA).

28. What controls are in place to prevent unauthorized access to personal information?

[redacted]

29. Please provide details on how you will track access to personal information.

Each type of user has access to the system/information based on the role they have. Audit reports are run to ensure there are no peculiarities in users interactions with files. This process is overseen by the Manager of Health and Wellness.

ARCHIVE INITIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

30. Describe the privacy risks for disclosure outside of Canada.

Use the table below to indicate the privacy risks, potential impacts, likelihood of occurrence and level of privacy risk. For each privacy risk identified, describe a privacy risk response that is proportionate to the level of risk posed.

This may include reference to measures to protect the sensitive personal information (contractual, technical, security, administrative and/or policy measures) that you outlined above.

Privacy risk	Impact to individuals	Likelihood of unauthorized collection, use, disclosure, or storage of PI (low, medium, high)	Level of privacy risk (low, medium, high)	Risk response (this may include contractual mitigations, technical controls and/or procedural and policy barriers)	Is there any outstanding risk? If yes, please describe.
[redacted]					

ACTIVE INITIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

ACTIVE INITIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

5 Data Linking

In FOIPPA, "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.

31. Does this initiative involve a program or activity that provides a service (or services) through a public body and at least one other public body or agency working collaboratively to provide that service?

☐ Yes ☑ No

32. Does this initiative involve a program or activity that provides a service (or services) through a public body that is working on behalf of one or more other public bodies or agencies?

☐ Yes ☑ No

33. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the Regulations? (Privacy Officer will answer).

☐ Yes ☑ No

ACTIVE INITIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

6 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 your personal information is safely secured in both physical and technical environments.

34. Does your initiative involve digital tools, databases information systems?

☑ Yes ☐No

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.

6.1 Security Safeguards

There are three broad types of security measures:

PHYSICAL	These security measures relate to the physical environment that the information is stored in; for example, whether your organization limits access to the filing cabinet or file room through select staff having a key.
TECHNICAL	Technical measures relate to your organization's hardware and software; for example, firewalls, encryption, and intrusion prevention systems.
ADMINISTRATIVE	Administrative controls are rules and processes for your employees or third parties that prevent them from inappropriately accessing, using, or disclosing your client's personal information; for example, role-based access controls, annual privacy training, employee codes of conduct, and privacy-related clauses in contracts.

ACTIVE INITIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

35. Describe administrative safeguards

[redacted]

36. Describe physical safeguards

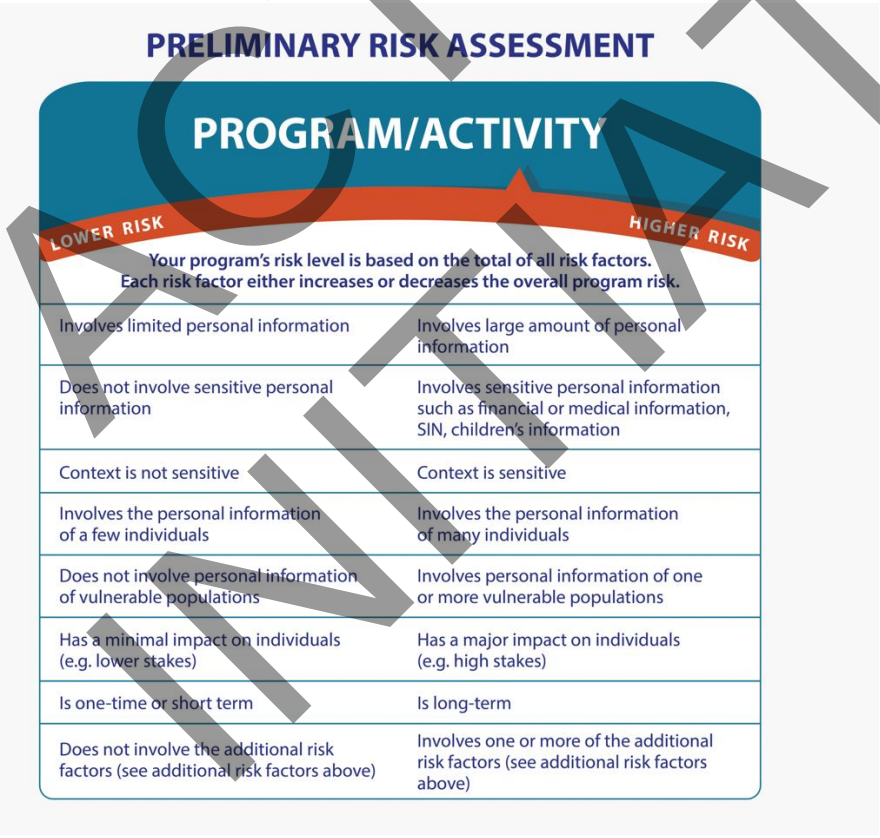
[redacted]

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

37. Please reach out to our CISO Office and ITS for the vendor assessments and technical requirements for IT/security threat risk assessment to fill out these sections or attach that assessment to this PIA.

HECVAT completed

7 Privacy Risk Identification and Mitigation



ACTIVE INITIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

38. 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.

*Risk Levels	Likelihood	Harm
Low	Little possibility that the risk will occur due to mitigating factors	Compromise would likely not result in any significant harm to the privacy, safety, or economic standing of individuals or the corporation.
Moderate	A possibility that the risk will occur if no additional measures are taken.	Compromise would likely cause some harm to the privacy, safety, or economic standing of individuals or the corporation.
High	Near certainty that the risk will occur in the future if no corrective measures are taken.	Compromise would likely cause significant and immediate harm to the privacy, safety, or economic standing of individuals or the corporation.

ACTIVE INITIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

RISK	MITIGATION STRATEGY	LIKELIHOOD	IMPACT
EXAMPLES Data that is no longer needed is at risk of being breached because it is being retained in the platform longer than is necessary	Implement a process on the IT platform to automatically delete data once is it no longer needed	Moderate	High
[redacted]			

ACTIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

[redacted]

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

[redacted]

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

[redacted]			

ACTIVE INITIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

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.

ACTIVE INITIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

8 Accuracy, Correction, and Retention

39. How will you make sure that the personal information is accurate and complete?

FOIPPA section 28 states that a public body must make every reasonable effort to ensure that an individual's personal information is accurate and complete.

Intake information is provided and entered by Student Service Representative (Medical Services) and Student Services Representative (Counselling Services) upon first contact for an appointment. It is written on a client information form and inputted into MOIS with either position. Provider does not go over that information at the first initial session.

We can set an alert for additional information needed on MOIS so whoever opens a patients file will be prompted to get the information and input (ex: PHN# alert).

40. Do you have a process in place to correct personal information?

☑ Yes ☐No

41. If yes, please describe your process below?

Client information is reviewed on intake and then reviewed upon returning (summer break or lapse in service (4 months)). Also, if someone is accessing Counselling Services and then decides to access Medical Services, due to patient being new to a clinic, it will be reviewed even if there is a chart in MOIS as they are seen as "new to Medical or new to Counselling"

ACTIVE INITIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

42. Sometimes it's not possible to correct the personal information. FOIPPA requires that you make a note on the record about the request for correction if you're not able to correct the record itself. Describe the process of how you will make a note on the record.

If we need to edit a encounter note, we add the date of the edit as a addition to note (entitled this) and why.

43. If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, FOIPPA requires you to notify the other public body or third-party recipient of the request for correction. How will you ensure that you conduct these notifications when necessary?

Once personal information correction is received we review the file to confirm if we have provided this information to someone else. If we have then we will contact that area again so they can update their information.

The provider, medical, would be the one who would revise the info and resend it to the 3rd party

Edits to encounter notes would be in encounter notes - for addresses or other, we do not have that noted.

44. 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

ACTIVE INITIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

- Using a person's health information to decide the level and type of care they receive

☐ Yes ☑No

45. If yes, do you have an approved information schedule in place related to personal information used to make decisions?

☑ Yes ☐No

46. If yes, please include your approved information schedule here.

Follow the College of Physician & Surgeons guidelines

Our current retention timeframe for retention of this information is 16 years from last visit/encounter

47. If you answered no, describe how you will ensure the information will be kept for a minimum of one year after it's used to make a decision that directly affects an individual.

ACTIVE INITIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

9 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

48. Will your initiative result in a personal information bank?

☑ Yes ☐No

If yes, answer the following questions, if "No" please proceed to the next section?

9.1 Description of personal information bank.

49. Name:

MOIS is a personal information bank

50. Location:

In cloud within Canada

ACTIVE INITIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

51. Description:

As above

52. 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).

as above 26(c)

53. Purpose:

As above

54. Category of Users:

MOIS has 9 categories to choose when setting up a security profile account that come with standard access points: Assessor, Counsellor, Doctor, Data Entry, MOA, Nurse, Resident, Supervisor and Systems Administrator. See below how we categorise our users in () :

Counsellor (Counsellor)
Practicum Counsellor (Counsellor)
Counselling Coordinator (Counsellor)
Counselling Service Representative (MOA)
Psychiatrist (Doctor)
Psychiatric Residence student (specialising student) (Resident)

ACTIVE INITIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

9.2 Method of De-identification/Anonymization/Aggregation for Personal Information

55. Please explain how Personal Information will be de-identified or anonymized and by whom?

General reporting is for overall usage of the services and the types of presenting issues so that we can ensure staff/resources are allocated to this area appropriately. This type of reporting is completed by the Manager of Wellness.

Report generated as a PDF not linked to identifiable individual client

9.3 Audits

56. 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?

[redacted]

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

57. Are the audit logs immutable?

[redacted]

58. Who reads the audit logs, and how long are they kept?

Overseen by the Manager logs are part of the overall system; reports are kept as long a needed to review and followup with users if an issue.

59. Who is responsible for oversight of user access?

Director approves all users to be added to our instance of MOIS; Manager approves role for each user once they are added to our instance.

60. 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?)

[redacted]

ACTIVE
TIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

61. 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?

[redacted]

62. Will those found to abuse access privileges be sanctioned in a meaningful (and visible) way?

YES - including suspension of access

ACTIVE INITIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

Privacy Impact Assessment Form

10 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: Moving MOIS to the Cloud

Position:
Acting Director of Wellness with significant input from the Manager of Wellness

I confirm the information management practices in this initiative have been documented 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: [redacted] Date: March 03, 23

March 3, 2023

ACTIVE INITIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

UNBC UNIVERSITY OF NORTHERN BRITISH COLUMBIA

Privacy Impact Assessment Form

Name of Director or Dean Overseeing the Program/Project:
Trevor Smith

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 [redacted] nge a PIA amendment if required.

Signature: [redacted] Date: March 3, 2023

Name of Chief Information Security Officer David Kubert

I confirm that this initiative to the best of my knowledge as written in the above sections, has information management practices that satisfactorily comply with the information security standards of the University of Northern British Columbia.

Signature: [redacted] Date: March 06, 2023

Name of Privacy Officer: Christopher Ross

Position: Governance Officer APRM

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

Signature: [redacted] Date: June 21, 2023

ACTIVE INITIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

11 APPENDIX A: 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.

ACTIVE INITIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

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

ACTIVE INITIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

	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: 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),

ACTIVE INITIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

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,
- 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.

ACTIVE INITIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

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.

ACTIVE INITIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18

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

ACTIVE INITIATIVE

COPY OF RECORD RELEASED JULY 31, 2024 IN RESPONSE TO FOI 24-18