Vancouver Island University

Telus Health Kroll Pharmacy Management Solution

Privacy Impact Assessment

Table of Contents

PART 1: GENERAL INFORMATION

PIA file number:

Initiative title:	Telus Health Kroll Pharmacy Management Solution
Organization:	Vancouver Island University
Branch or unit:	Pharmacy Technician Diploma Program
Your name and title:	Jo-Ann Bellamy, Privacy Consultant
Your work phone:	250-208-3431
Your email:	jbellamy@hooperconsulting.ca

Initiative Lead name and title:	Patricia O'Hagan Dean, Faculty of Health Sciences and Human Services
Initiative Lead phone:	250-740-6241
Initiative Lead email:	Patricia.O'Hagan@viu.ca
Privacy Officer:	William Boyte General Counsel and University Secretary
Privacy Officer phone:	250-740-6564
Privacy Officer email:	William.boyte@viu.ca

General information about the PIA:

Is this initiative a data-linking program under FOIPPA? If this PIA addresses a data-linking program, you must submit this PIA to the Office of the Information and Privacy Commissioner.
No
Is this initiative a common or integrated program or activity? Under section FOIPPA 69 (5.4), you must submit this PIA to the Office of the Information and Privacy Commissioner.
No
Related PIAs, if any:
None

1. What is the initiative?

Describe your initiative in enough detail that a reader who knows nothing about your work will understand the purpose of your initiative and who your partners and other stakeholders are. Describe what you're doing, how it works, who is involved and when or how long your initiative runs.

Vancouver Island University (VIU) is a public university on the west coast of Canada with campuses on the traditional territory of the Suneymuxw, Quw'utsun, Tla'amin, Snaw-naw-as

and Qualicum First Nations. VIU offers more than 120 programs, from graduate and undergraduate degrees to trades diplomas and certificates. VIU has approximately 12,000 students (12% Indigenous and 12% international) and 1500 faculty and staff.

VIU's Pharmacy Technician Program includes a course in which students are trained in the use of pharmacy technology platforms that are commonly used by pharmacies in Canada. This PIA is assessing one of these platforms, the Telus Health Kroll Pharmacy Management Solution (Kroll). Kroll is a customizable solution that supports the needs of pharmacies by improving operational efficiencies, encouraging patient engagement, and improving dispensing workflow. Kroll also helps pharmacies reduce the potential for dispensing errors with built-in adverse drug event detection, support for allergies and medical conditions, and barcode scan verification.

Students will be trained on Kroll to ensure they are proficient in the platform before being placed in a co-op or being hired at a pharmacy. Students will not use live patient information in Kroll but will instead build fictitious doctor and patient files. The Kroll solution will be used within VIU only and will not adjudicate or communicate with any outside entities.

The instructor (or staff member in charge of setting up the Kroll accounts) will enter the student's first and last initials for their username (and occasionally middle initials if two students have the same first and last initials). Students will be prompted to create their own password when they log into Kroll for the first time.

Kroll will be used at VIU for training purposes only. When a student is placed in a pharmacy for a co-op term, the student will use the pharmacy's platform and will be covered by the pharmacy's privacy practices. Each pharmacy and health authority has their own privacy and confidentiality document that the student will sign and agree to.

2. What is the scope of the PIA?

Your initiative might be part of a larger one or might be rolled out in phases. What part of the initiative is covered by this PIA? What is out of scope of this PIA?

This PIA addresses the collection, use, disclosure, storage, and security of personal information in the Telus Health Kroll Pharmacy Management Solution that will be used as a training tool at

Vancouver Island University. The personal information will include student initials and passwords only.

This PIA does not include the use of Kroll when a student is on a co-op term with a pharmacy.

3. 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.

The personal information includes students' first and last initials and password.

No patient or other individual's personal information will be collected or used in Kroll.

3.1 Did you list personal information in question 3?

Personal information is any recorded information about an identifiable individual, other than business contact information. Personal information includes information that can be used to identify an individual through association or reference.

Yes.

- If yes, go to Part 2
- If no, answer question 4 and submit questions 1 to 4 to your Privacy Officer. You do not need to complete the rest of the PIA template.

4. How will you reduce the risk of unintentionally collecting personal information?

Some initiatives that do not require personal information are at risk of collecting personal information inadvertently, which could result in an information incident.

N/A

PART 2: COLLECTION, USE AND DISCLOSURE

This section will help you identify the legal authority for collecting, using and disclosing personal information, and confirm that all personal information elements are necessary for the purpose of the initiative.

5. Collection, use and disclosure

Use column 2 to identify whether the action in column 1 is a collection, use or disclosure of personal information. Use columns 3 and 4 to identify the legal authority you have for the collection, use or disclosure.

Use this column to describe the way personal information moves through your initiative step by step as if you were explaining it to someone who does not know about your initiative.	**Collection, use or disclosure**	**FOIPPA authority**	**Other legal authority**
Step 1: Instructor creates student's account username using first and last initials (and occasionally middle initials). Students create their own passwords.	Collection	S. 26	
Step 2: Students log in to Kroll using their username and password.	Use	S. 32(a) and 32(b)	
Step 3: The student's work in Kroll is used by the instructor to evaluate the student.	Use	S. 32(c)	

6. Collection Notice

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

VIU

Students are provided with a collection notice when they register to become a student at VIU. The collection and use of student personal information in Kroll is consistent with the purpose outlined in the collection notice.

Telus Health Kroll

Telus Health's Privacy Policy which includes a collection notice can be found at https://www.telus.com/en/health/about-telus-health/privacy?linktype=ge-footer

PART 3: STORING PERSONAL INFORMATION

If you're storing personal information outside of Canada, identify the sensitivity of the personal information and where and how it will be stored.

7. Is any personal information stored outside of Canada?

No.

8. Does your initiative involve sensitive personal information?

No.

- If yes, go to question 9
- If no, go to question 10

9. Is the sensitive personal information being disclosed outside of Canada under FOIPPA section 33(2)(f)?

N/A

- If yes, go to question 10
- If no, go to Part 4

10. Where are you storing the personal information involved in your initiative?

Personal information in Kroll is stored in Telus Health's data centres located in Canada. No personal data is accessed from outside Canada.

After you answer this question go to Part 5.

PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

Complete this section if you are disclosing sensitive personal information to be stored outside of Canada. You may need help from your organization's Privacy Officer.

11. Is the sensitive personal information stored by a service provider?

N/A

- If yes, fill in the table below (add more rows if necessary) and go to question 13
- If no, go to question 12

Name of service provider	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?
N/A		

12. Provide details on the disclosure, including to whom it is disclosed and where the sensitive personal information is stored.

N/A

13. Does the contract you rely on include privacy-related terms?

N/A

- If yes, describe the contractual measures related to your initiative.

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

N/A

16. Provide details about how you will track access to sensitive personal information.

N/A

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

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

N/A

Privacy risk	Impact to individuals	Likelihood of unauthorized collection, use, disclosure or storage of the sensitive personal information (low, medium, high)	Level of privacy risk (low, medium, high, considering the impact and likelihood)	Risk response (this may include contractual mitigations, technical controls, and/or procedural and policy barriers)	Is there any outstanding risk? If yes, please describe.
N/A					

Outcome of Part 4

The outcome of Part 4 will be **a risk-based decision made by the head of the public body on whether to proceed with the initiative**, with consideration of the risks and risk responses, including consideration of the outstanding risks in question 17. **The public body may document the decision in an appropriate format as determined by the head of the public body or by using this PIA template.**

PART 5: SECURITY OF PERSONAL INFORMATION

In Part 5 you will share information about the privacy aspect of securing personal information. People, organizations or 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.

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

Yes.

- If yes, work with your Privacy Officer to determine whether you need a security assessment to ensure the initiative meets the reasonable security requirements of FOIPPA section 30

18.1 Do you or will you have a security assessment to help you ensure the initiative meets the security requirements of FOIPPA section 30?

No.

- If yes, you may want to append the security assessment to this PIA. Go to question 20
- If no, go to question 19

19. What technical and physical security do you have in place to protect personal information?

VIU – Physical:

- Manager of Security is contracted for security services, however additional on-site services are provided by an external security company who provide a 24/7 security presence and monitoring services.
- Exterior building doors are locked at night and open to the public during the day. Some interior entrances to office areas are also locked during daytime and not open to the public.
- Security system provides audit trails on facility accesses.
- Individual offices are locked with limited access.
- Building intrusion detection system is in place.
- Confidential destruction bins and services are in place.
- [redacted] clinic is closed, and clinic doors are locked on timed schedule. s. 15(1)(l)
- [redacted]
- [redacted]
- A closed-circuit television system is in use at all campuses.

VIU – Technical:

[redacted]

- Backups are encrypted.

[redacted]

- User access is limited, based on "need to know" principles. No standard or scheduled reviews are in place to ensure accesses are accurate and complete.
- Employees may not remove personal information from the physical office site which includes the use of portable drives and desktop storage on laptops. s. 15(1)(l)
- [redacted]
- [redacted]

Telus Health

Telus Health maintains an information security governance program to protect personal information. Telus Health, in compliance with its security policy and data centre security standard, employs security measures appropriate to the sensitivity of the information in an effort to protect personal information against such risks as loss or theft, unauthorized access, disclosure, copying, use, modification or destruction.

Security measures include but are not limited to the following:

- Using appropriate administrative, physical and technical security controls designed to prevent and detect unauthorized access to personal information
- Employing encryption for data at rest and in transit, tokenization, de-identification and other mechanisms to protect personal information as appropriate
- Limiting access to the data to a need-to-know basis and applying the principles of least privilege and role-based access control
- Requiring secure disposal of any media containing personal information
- Prohibiting the use of personal information in non-production or demonstration environments except with the express consent of the Customer
- Implementing a Secure by Design methodology in work processes

- Identifying and assessing reasonably foreseeable risks to the integrity, confidentiality or availability of personal information and taking reasonable steps to mitigate those risks through the implementation of safeguards
- Regular testing of safeguards and overall security program

Telus Health protects personal information shared with service providers by employing contractual or other means to ensure that any such service provider will provide a comparable level of protection while personal information is being processed by that service provider.

Telus Health employment agreements include contractual provisions for the safeguarding and proper usage of confidential information (including personal information) accessible to employees in the course of their employment. Telus Health will take appropriate disciplinary measures where necessary to enforce their Privacy Policy.

20. Controlling and tracking access

Please check each strategy that describes how you limit or restrict who can access personal information and how you keep track of who has accessed personal information in the past. Insert your own strategies if needed.

Strategy	
We only allow employees in certain roles access to information	Yes
Employees that need standing or recurring access to personal information must be approved by executive lead	N/A
We use audit logs to see who accesses a file and when	N/A
Describe any additional controls:	

PART 6: ACCURACY, CORRECTION AND RETENTION

In Part 6 you will demonstrate that you will make a reasonable effort to ensure the personal information that you have on file is accurate and complete.

21. 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.

The instructor (or staff member in charge of setting up Kroll accounts) enters the student's initials to create a user account. Students create their own passwords.

22. Requests for correction

FOIPPA gives an individual the right to request correction of errors or omissions to their personal information. You must have a process in place to respond to these requests.

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

Students can change their personal information (e.g., their initials for login) by contacting the instructor or staff member who set up their account.

22.2 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. Will you document the request to correct or annotate the record?

N/A

22.3 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 of the request for correction. Will you ensure that you conduct these notifications when necessary?

N/A

23. Does your initiative use personal information to make decisions that directly affect an individual?

Yes, the student's work in Kroll is used by the instructor for evaluation purposes.

- If yes, go to question 24
- If no, skip ahead to Part 7

24. Do you have an information schedule in place related to personal information used to make a decision?

FOIPPA requires that public bodies keep personal information for a minimum of one year after it is used to make a decision. In addition, the Information Management Act requires that you dispose of government information only in accordance with an approved information schedule.

Yes.

- If 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.

PART 7: AGREEMENTS AND INFORMATION BANKS

Please provide information about whether your initiative will involve an information sharing agreement, research agreement or personal information bank.

25. Does your initiative involve an information sharing agreement?

No.

- If yes, please complete the Information Sharing Agreement Supplement and attach it to your PIA

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

A personal information bank (PIB) is a collection of personal information searchable by name or unique identifier.

No.

- If yes, please complete the table below.

Describe the type of information in the bank:
Name of main organization involved:
Any other ministries, agencies, public bodies, or organizations involved:
Business contact title and phone number for person responsible for managing the PIB:

PART 8: ADDITIONAL RISKS

Part 8 asks that you reflect on the risks to personal information in your initiative and list any risks that have not already been addressed by the questions in the template.

27. Risk response

Describe any additional risks that arise from collecting, using, storing, accessing, or disclosing personal information in your initiative that have not been addressed by the questions on the template.

Possible risk	Response
Risk 1: Unauthorized individuals at VIU access the personal information in Kroll.	Access to student information in Kroll is limited to authorized instructors and IT personnel only. All employees are required to comply with FOIPPA. VIU has privacy policies and protocols in place to ensure the security of personal information.
Risk 2: Real personal information is input into Kroll when creating patient records for training purposes.	VIU and students use fictitious information when building doctor and patient files in Kroll. There are a limited number of fictitious records that are used for training purposes only.
Risk 3: Unauthorized individuals at Telus Health access the personal information in Kroll	Telus Health has a Privacy Management Program in place which includes privacy policies and protocols. Access to data is on a need-to-know basis with the principles of least privilege and role-based access control applied. Employees undergo mandatory annual privacy training. Employment agreements include contractual provisions for the safeguarding and proper usage of confidential information (including personal information) accessible to

Possible risk	Response
	employees in the course of their employment. Telus Health takes appropriate disciplinary measures where necessary to enforce their Privacy Policy.
Risk 4: Personal information is compromised during transmission.	Telus Health employs encryption for data at rest and in transit, tokenization, de-identification and other mechanisms to protect personal information.
Risk 5: Personal information disclosed to service providers under contract to Telus Health is compromised.	Telus Health protects personal information shared with service providers by employing contractual or other means to ensure that any such service provider will provide a comparable level of protection while personal information is being processed by that service provider.

PART 9: SIGNATURES

You have completed a PIA. Submit the PIA to your Privacy Officer for review and comment, and then have the PIA signed by those responsible for the initiative.

Privacy Office Comments

Privacy Office Signatures

This PIA is based on a review of the material provided to the Privacy Office as of the date below.

Role	Name	Electronic signature	Date signed
Privacy Officer / Privacy Office Representative	Bev Hooper Hooper Access and Privacy Consulting L	[redacted] s. 22(1)	Mar 3/23

Program Area Signatures

This PIA accurately documents the data elements and information flow at the time of signing. If there are any changes to the overall initiative, including to the way personal information is collected, used, stored, or disclosed, the program area will engage with their Privacy Office and if necessary, complete a PIA update.

Program Area Comments:

Role	Name	Electronic signature	Date signed
Initiative lead	Patricia O'Hagan Dean, Faculty of Health Sciences and Human Services		
Head of public body, or designate	William Boyte General Counsel and University Secretary		