Privacy Impact Assessment (PIA) for UbiSim

Before you start 1
PART 1: GENERAL INFORMATION 2
PART 2: COLLECTION, USE, AND DISCLOSURE 5
PART 3: STORING PERSONAL INFORMATION 7
PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA 7
PART 5: SECURITY OF PERSONAL INFORMATION 10
PART 6: ACCURACY, CORRECTION AND RETENTION 11
PART 7: PERSONAL INFORMATION BANKS 13
PART 8: ADDITIONAL RISKS 13
PART 9: SIGNATURES 14

Before you start

- This Privacy Impact Assessment (PIA) form is used by VCC to assess whether a new initiative, or proposed significant change to an existing initiative, meets the privacy protection requirements of the B.C. *Freedom of Information and Protection of Privacy Act.* FIPPA's protection of privacy requirements. A PIA is a legislative requirement (FIPPA s. 69(5.3)) and mandatory before implementing an initiative.
- You/Your refers to the individual responsible for drafting this PIA, who should be an individual from the relevant department or program area with sufficient knowledge to do so. The PIA must be signed by the role within the program area with the appropriate position to hold accountability for this initiative.
- Please include references to other documents when applicable, but do not insert or embed any documents to/in this assessment form.

PART 1: GENERAL INFORMATION

PIA file number: 2025-008

Initiative title:	Nursing VR software (UbiSim)
VCC Department / Program Area:	School of Health Sciences
Link to VCC initiative website:	n/a
Link to vendor website:	https://www.ubisimvr.com
Link to vendor privacy policy:	https://www.labster.com/privacy-policy/
Your name and title:	Dustin Chan, Manager of Simulation and Experiential Learning
Your work phone and email:	604-871-7675, dchan@vcc.ca
Initiative Lead name and title:	Same as above
Initiative Lead phone and email:	Same as above

General information about the PIA:

Is this initiative a data-linking program under FIPPA? See the definition in Schedule 1 of FIPPA. If this PIA addresses a data-linking program, the Privacy Officer must submit this PIA to the Office of the Information and Privacy Commissioner.	No
Is this initiative a common or integrated program or activity? See the definition of Schedule 1 of FIPPA. Under section FIPPA 69 (5.4), the Privacy Officer must submit this PIA to the Office of the Information and Privacy Commissioner.	No
Does this initiative involve a regular or systematic exchange of personal information between organizations? If yes, this initiative may require an Information Sharing Agreement.	No
Related PIAs, if any: N/A	

1. What is the initiative?

UbiSim by Labster is an immersive virtual reality simulation platform designed to support nurses' clinical education. This is license subscription for UbiSim for the implementation of a pilot project for our Practical Nurse and Bachelor Science Nursing program and to our Health Care assistant program as well. This software will be implemented through a strategic pilot project targeting a select group of nursing students. The initiative will involve carefully aligning VR scenario objectives with specific course learning

outcomes, utilizing a combination of pre-made and customized scenarios. The VR technology will be integrated with existing simulation modalities, such as high-fidelity mannequins and standardized patients, to create a comprehensive and enhanced learning experience. Following best practices in simulation implementation, all participating nursing students will engage with the VR scenarios, followed by formal debriefing sessions.

UbiSim has a repository of scenarios that faculty will assign students to engage in. The students will be playing the scenarios either on their own or in groups, working as a team to complete the VR scenarios objectives. Once the scenario is complete, data about performance within the scenario will auto-populate that is available for students to review their achievements. This data will be used to encourage repeat gameplay improve outcomes or a copy may be extracted to aid them in self or instructor led reflection depending on learning objectives. The number of scenarios that students can engage in per term will vary depending on faculty member and what is assigned to the learners based on course learning objectives. Faculty will work with the experiential learning team to offer more time to practice and repeat the gameplay to improve their outcomes.

To ensure smooth integration and implementation, change management principles will be applied, including a champions model for faculty training and the establishment of peer-to-peer support systems. Additionally, the software will be introduced to students at the beginning of their program and consistently incorporated throughout their studies, allowing them to become familiar with its functionality and expectations, ultimately supporting their orientation and ongoing educational journey.

UbiSim enhances student engagement and learning outcomes through innovative, immersive experiences that align with the expectations of modern learners who are accustomed to advanced educational technologies seen in K to 12. The implementation of VR as a complementary simulation modality alongside traditional methods like mannequins and standardized patients creates a more comprehensive and effective experiential learning environment. This approach prepares students for the increasing use of VR training in professional healthcare settings giving them foundational knowledge within their programs. VR also keeps the institution competitive in attracting prospective nursing students.

Furthermore, the software can provide a long-term cost savings and environmentally friendly alternative to just traditional nursing skills practice. It lowers the need for expensive consumable supplies, which typically cost students around $250 per kit, by utilizing virtual assets that can be reused indefinitely without additional cost or environmental impact. This virtual approach also allows for standardized, repeatable training scenarios that may be difficult or resource intensive to recreate in a real-life setting, particularly for rare or critical events.

Lastly, the software pilot can help to addresses the challenge of limited clinical placement opportunities by offering scalable, immersive experiences that can supplement or partially replace traditional clinical training. This helps to ensure that nursing students receive consistent experiences, especially when real-world opportunities may be limited or variable based on the specific location, time and patient opportunity such as experience with a patient heart attack or fall.

2. What is the scope of the PIA?

This PIA covers the collection, use, and disclosure of personal information by UbiSim during its operations in VCC's Practical Nurse, Bachelor Science Nursing, and Health Care Assistant programs, for academic use only.

This PIA does not cover the mobile device management solution that is needed to support the VR headsets required for the UbiSim software. s. 13(1), s. 17(1) .

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

Accounts/licence: Student name (first, last), VCC student email, educational affiliation (VCC)

Within software: UbiSim processes and creates an assessment of the learner's performance of the scenario by reviewing the learner's performance within the simulation but not recording it.

UbiSim stores this learning assessment and it can be accessed by the student and can be shared with the faculty member for the purposes of feedback and reflection. This assessment is not graded as it is a formative learning experience that gives thoughtful feedback for improvement. Data is collected about each individual student's performance only. There is no synthesis of data sets and data is not used to train any models in any way.

User data: Use of cloud-based software may also collect application or site usage data (visits, sessions, downloads); browser or device profile (type, OS, language, resolution, apps, etc.); browsing history; IP address; device ID; geolocation data; browser data and files (such as cookies, pixels, strings, and browser fingerprint). Students will access UbiSim via VCC owned VR headsets located on campus and so UbiSim will not collect this information about students individually. This may need to be reassessed if a loaner program is introduced.

UbiSim has the capability to collect voice recordings during the simulation play but VCC will not enable this feature at this time.

3.1 Did you list personal information in question 3?

Yes

- If yes, are all of the personal information elements **necessary** for your initiative?
    - Yes

4. If you answered "no" to question 3.1: How will VCC 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 a privacy breach or other privacy incident. After you answer this question, submit this PIA to the Privacy Office. You do not need to complete the rest of the PIA template.

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 flow

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**	**FIPPA authority or other legal authority**	**Specify any potential risks**
Names and emails for participating students are collected by internal support staff to populate a spreadsheet.	Collection	26(c)	
Internal support staff will then upload collected names and emails into the software to assign each of the students to their own student license using their email to register and login. Faculty are also assigned licence to access as instructor.	Use	32(a)	
Faculty use UbiSim like an LMS to create learning activities and assign students to scenarios using their email IDs. Students will use their emails to login to engage in the learning activity.	Use	32(a)	

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	FIPPA authority or other legal authority	Specify any potential risks
Students log in to UbiSim and engage in learning activities; UbiSim collects information about the students' performance in each learning scenario or activity.	Use Collection	32(a) 26(c)	
Once activity is completed, UbiSim automatically generates performance feedback/assessment based on the learning experience. This feedback is retained on the cloud-based server and can be accessed and reviewed only by the individual student or faculty member, and can be saved as PDF/printed. Faculty may review results with learners but performance feedback is not graded, used for assessment, or disclosed unless with student's consent to other faculty.	Use Disclosure	32(a) 33(2)(c)	

Information security flow table available from UbiSim here:

s. 15(1)(l)

6. Collection Notice and Consent

6. 1 Collection Notice

Collection notice:

Your personal information is collected under the authority of s. 26(c) of the BC *Freedom of Information and Protection of Privacy Act* (FIPPA). This information will be used to assign you a UbiSim licence and to assess and provide feedback on your performance in the learning activity. Questions about the collection of this information may be directed to VCC School of Health Sciences, Dustin Chan, Manager of Simulation and Experiential Learning, dchan@vcc.ca.

Location: The collection notice will be provided in the course syllabus and student learning guides. It will also be included in prebrief presentations prior to simulation activities at VCC SHS's simulation and experiential learning center.

6. 2 Consent

N/A

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?

Yes

8. If you answered yes to Question 7: Where are you storing the personal information involved in your initiative?

UbiSim's data center is hosted at AWS, USA s. 15(1)(l) AWS data center is ISO27001 certified.

9. Does your initiative involve sensitive personal information that will be stored outside of Canada?

No.

- If yes, go to question 10
- If no, skip ahead to Part 5

10. If you answered "yes" to Question 9: Is the sensitive personal information being stored outside of Canada only because it is being made available to the public under an enactment that authorizes or requires the information to be made public (FIPPA section 33(2)(f))?

[Answer: Yes or No]

- If yes, what enactment?
  - [Answer] then skip ahead to Part 5.
- If no, go to Part 4.

PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

Complete this section **only if you answered yes to Question 9: you are disclosing sensitive personal information to be stored outside of Canada**. This section will require consultation with a representative from IT Services.

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

[Answer: Yes or No]

- If yes, fill in the table below (add more rows if necessary) and then 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)?

12. If you answered "no" to Question 11: Provide details on the disclosure, including to whom it is disclosed and where the sensitive personal information is stored.

[Answer]

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

[Answer: Yes or No]

- If yes, describe the contractual measures related to your initiative.
  - [Answer]
- Is VCC's Privacy Protection Schedule or Privacy Protection Schedule for Cloud Services appended to the initiative's contract? [Answer: Yes or No]

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

[Answer]

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

[Answer]

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

Privacy risk	Impact to individuals (low, medium, high)	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.

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 and/or your vendor need to make sure that the personal information is safely secured in both physical and technical environments.

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

Yes

- If yes: Are these digital tools, databases, or information systems new to VCC?
    - Yes

17.1 If you answered "yes" to Question 17: Do you or will you have a security assessment to ensure the initiative meets the security requirements of FIPPA s. 30?

Yes – IT Services has assessed and approved UbiSim.

- If yes, go to question 19. If you have or will complete a security assessment during the development of your initiative, you do not need to answer the question about technical security.

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

Describe where the records, whether digital or physical, for your initiative are stored (e.g., on your organization's LAN, on your computer desktop, in a filing cabinet, etc.) and the technical and/or physical security measures in place to protect those records. (Please consult the policies for any software/cloud services/etc. but please do not just copy and paste).

- *Technical security measures include secure passwords, encryption, firewalls, etc.*
- *Physical security measures include restricted access to filing cabinets or server locations, locked doors, security guards, etc.*

N/A - IT has completed the security assessment and approved. UbiSim is SOC 2 Type 2 compliant.

19. Controlling and tracking access

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 their managerial lead:	Yes: Manager of Simulation and Experiential Learning will approve requests and administer faculty login accounts. These accounts only receive access to their prescribed sections and their student cohorts.
We use audit logs to see who accesses a file and when:	No
Describe any additional controls:	Logging into the software requires personal access and several step authentication process to access the class' information. Only faculty members teaching with the tool will have access.

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.

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

Student name and students' VCC email addresses are provided by faculty from class lists. Students will be sent in a confirmation email once their licence is assigned that will give them access to register and login to UbiSim platform.

The student data gained from the learning activity about the performance is automatically created by UbiSim's generated assessment of the learning activity. The data generated about performance cannot be manipulated and will be based on performance. No other data is collected. This data stays on the cloud-based server and accessed by the student and faculty only.

21. Requests for correction

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

Learning activities cannot be corrected and contact information is taken from class list and can be edited. Data within UbiSim can be deleted.

- If yes: Please describe the process.
    - We can removed access of the student's email address and delete performance results of the learning activity when logged in as an administrator or faculty member.
    - VCC can also request the deletion of data from UbiSim.

21.2 Sometimes it's not possible to correct the personal information. FIPPA s. 29 requires that you make a note on the record about the request for correction if you are not able to correct the record itself. Will you document the request to correct or annotate the record?

N/A

21.3 If you receive a request for correction from an individual and you know you disclosed their personal information in the last year, FIPPA s. 29 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 – No disclosure of personal information to public body or third party.

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

Students are not directly assessed or graded on any of their performance in UbiSim. Students may be asked to write reflections on their experience as part of assessment within the course but UbiSim's assessment feedback will not directly contribute to this.

23. If you answered "yes" to Question 22: Do you have a records retention schedule in place related to personal information used to make a decision?

N/A

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

  Information in UbiSim is not used to make decisions that directly affect individuals, but it will be deleted at the year end when licences are wiped and re-assigned to other students.

PART 7: PERSONAL INFORMATION BANKS

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

No.

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.

25. Risk response

Possible risk	Response / mitigation strategies
Students or faculty members share their personal password and access with others	General password protection processes; Students and faculty required to follow VCC Policy 505 Appropriate and Responsible Use of Educational and Information Technology

Possible risk	Response / mitigation strategies
Faculty share students' feedback and learning outcomes with other faculty who do not have a reason to access this information.	Faculty follow VCC FIPPA policy and legislation; Faculty request students' consent to share feedback from UbiSim with other faculty if there is an interest.
UbiSim learning activity assessment/feedback is used in assessing or grading students.	PIA should be updated to reflect that UbiSim is collecting PI to be used to make a decision that directly affects an individual.
VCC enables UbiSim voice recording feature in simulations.	PIA may need to be revised to reflect new feature and associated risks.

PART 9: SIGNATURES

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

Privacy Office Comments

This PIA considers the current/proposed use of UbiSim software in the School of Health Sciences Simulation Centre. Part 8 identifies some additional risks that should be addressed if the current collection or use of personal information changes, especially in relation to these aspects.

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	Caralee Maloney	Caralee Maloney Digitally signed by Caralee Maloney Date: 2025.06.11 13:05:29 -07'00'	June 11, 2025

Program Area Signatures

The PIA must be signed by a role that is able to hold accountability for a PIA, proportionate to the sensitivity of personal information and/or the risks of the initiative. This signature confirms that this PIA accurately documents data elements and information flow at the time of signing. If there are any

changes to the overall initiative, including the way personal information is collected, used, stored, or disclosed, the program area will contact Privacy and, if necessary, complete a PIA update.

Program Area Comments:

Role	Name/Position	Electronic signature	Date signed
Role designated accountable for the initiative	Dustin Chan, Manager of Simulation and Experiential Learning	Dustin Chan Digitally signed by Dustin Chan Date: 2025.06.13 16:10:26 -07'00'	June 13, 2025
Contact Responsible for Systems Maintenance and/or Security	Norman Chang	Norman Chang Digitally signed by Norman Chang Date: 2025.06.12 12:42:12 -07'00'	June 12, 2025