Vancouver Island University

Dentrix

Privacy Impact Assessment

Table of Contents

PART 1: GENERAL INFORMATION

PIA file number:

Initiative title:	Dentrix, Henry Schein One
Organization:	Vancouver Island University
Branch or unit:	Dental Clinic
Your name and title:	Jarod Hooper, Hooper Access and Privacy Consulting Ltd. (HAPC)
Your work phone:	250-588-8055
Your email:	jarod@hooperconsulting.ca

Initiative Lead name and title:	Patricia O'Hagan, Dean of Health Sciences and Human Services
Initiative Lead phone:	250-740-6241
Initiative Lead email:	Patricia.ohagan@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 Dental Clinic program is assessing Dentrix, a dental software owned by Henry Schein Practice Solutions, Inc. Dentrix is a central practice management software that leads the dental software market by providing solutions for both the clinical and business sides of practice. VIU is assessing the clinical product, which they will use in the classroom to train students who are entering the dental field. Dentrix' clinical software supports many features such as Dentrix Smart Image, Dentrix 3D Patient Charting, Dentrix Perio Chart, and Digital Dental Exchange. In addition to those features, users may also use Dentrix to synchronize digital images with patient records, organize clinical notes, and submit and monitor lab cases digitally.

Students are trained on Dentrix to ensure they are proficient in the platform before being hired at a dental practice. Students will use live patient information in Dentrix. The Dentrix solution will be used within VIU [redacted] No employees at Dentrix or Henry Schein Practices, Inc. will have access to any personal information inputted by VIU. s. 15(1)(l)

Students who are registered in the dental program are given a unique username and password to access Dentrix. [redacted] s. 15(1)(l)

VIU hosts the opportunity for individuals to apply to become a Client at their Dental Clinic. Clients are required to provide health history and to sign a consent form. Payment for the Client program is facilitated using Moneris, a third-party payment processor. The consent form collects name, city, and signature [redacted] Personal information inputted into Dentrix includes first and last name, preferred name, home address, phone number, email address and birthdate. Personal information also includes the health and dental history of the client, as well as any radiographs captured by SafeCom in the Clinic. s. 15(1)(l)

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 Dentrix platform that will be used as a training tool at Vancouver Island University.

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.

Student personal information is limited to username and password.

Client personal information collected from the consent form includes full name, city, and signature. Client personal information manually entered into Dentrix includes full name, preferred name, home address, phone number, email address and birthdate. Personal information also includes the health and dental history of the client, including radiographs captured in the Clinic.

Moneris only collects payment information as necessary to complete the transaction. This information includes name, credit card number, billing address, email address, telephone number, and birthdate. VIU collects no payment information from the Client other than their corresponding receipt number from the transaction which is added to their chart.

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.

Inadvertent collection is not anticipated as students will use Dentrix under the supervision of their instructor. Students will use the username and password provided by their instructor to access Dentrix. Client information is only inputted into Dentrix after client written consent is given.

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 an individual student username and password for each student in their class. [redacted]	Collection	S. 26(c)	
Step 2: An individual contacts VIU to apply to become a Client. Clients sign a consent form which collects full name, city and signature.	Collection	S. 26(c)	

s. 15(1)(l)

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
When they have been accepted, clients provide their full name, preferred name, home address, phone number, email address, birthdate, medical and oral health history. Payment information collected by Moneris includes name, credit card number, billing address, email address, telephone number, and birthdate.			
Step 3: Students log in to Dentrix using their username and password.	Use	S. 32(a) and 32(b)	
Step 4: Clients receive dental care from students and faculty and is recorded in Dentrix.	Collection Use	S.26(c) S. 32(a) and 32(b)	
Step 4: The student's work in Dentrix is used by the instructor to evaluate the student.	Use	S. 32(c)	
Step 5: Radiographs captured by SafeCom are shared with the Client's personal dentist. The dentist receives the records using an encrypted email system.	Disclosure	S. 33(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).

The information on this form is collected for the purpose of providing dental services at Vancouver Island University. The personal information is collected under the authority of the *University Act* and is subject to the *Freedom of Information and Privacy Act*. Your personal information including radiographic images will be shared with your personal dentist. If you have any questions about the collection and use of your information, contact (name of contact, email, phone number).

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?

Yes.

- 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

s. 15(1)(l)

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

[redacted]

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?

[redacted] s. 15(1)(l)

- 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)?
[redacted]		

s. 15(1)(l)

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

Student personal information is disclosed to all faculty in the dental department. Client personal information is disclosed to necessary VIU students and faculty in the dental department. Radiographs captured using SafeCom are shared with the Client's personal dentist.

[redacted] s. 15(1)(l)

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

13.

N/A.

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

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

User access is based on least privilege principles. Access to the software is limited to only authorized individuals/students. Dentrix software is only on computers in the Dental Clinic.

[redacted]

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

s. 15(1)(l)

Username and password are given only to the individual student. [redacted]

[redacted]

16. 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.

17. 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

17.1 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

18. 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 doors are locked on timed schedule.
- [redacted]
- [redacted]
- A closed-circuit television system is in use at all campuses.

s. 15(1)(l)

VIU – Technical:

- [redacted]
- [redacted]
- Backups are encrypted.

- [redacted]

s. 15(1)(l)

- 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.
- [redacted]

s. 15(1)(l)

- [redacted]

Dentrix – Technical:

s. 15(1)(l); s. 21(1)

Data Protection: [redacted]

Integrations: [redacted]

Active Directory Integration: [redacted]

Disaster Recovery: [redacted]

Industry Certifications: [redacted]

19. 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	Yes
Describe any additional controls:	Faculty are given access as they are directly connected to the teaching of the students in both programs. Students record name and initials on all client entries in the paper chart. Faculty initials charts when marking student work and the software records initials of all entries. Dentrix software includes audit logs.

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?

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 Dentrix) assigns each student a username and password. Students and faculty complete chart audits.

21. 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.

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

Yes.

21.2 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.

21.3 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.

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

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

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

23. 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.

VIU keeps information on file as per their regulatory body, British Columbia College of Oral Health Professionals.

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.

24. Does your initiative involve an information sharing agreement?

No.

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

25. 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.

Yes

- If yes, please complete the table below.

Describe the type of information in the bank: full name, preferred name, home address, phone number, email address, birthdate, payment receipt, health and dental history of the client, including radiographs captured by SafeCom in the Clinic.
Name of main organization involved: Vancouver Island University Dental Clinic
Any other ministries, agencies, public bodies, or organizations involved: No
Business contact title and phone number for person responsible for managing the PIB: Patricia O'Hagan, Dean, Health Sciences and Human Services, 250-740-6241

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.

26. 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
Unauthorized individuals at VIU access the personal information and use it for unauthorized purposes.	Access is restricted based on least privilege and need-to-know principles. Students adhere to Standard 7.0: Confidentiality noted in their student handbook.
Unauthorized individuals at Dentrix or Henry Schein One Inc. access the personal information and use it for unauthorized purposes.	No employees at Dentrix or Henry Schein One have access to VIU's data. [redacted]
Radiographs captured by SafeCom are intercepted during transmission from VIU to the Client's personal dentist.	[redacted]

s. 15(1)(l)

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 Ltd.	[redacted]	March 15/23

s. 22

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 of Health Sciences and Human Services		
Program/Department Manager			
Head of public body, or designate Only required if personal information is involved	William Boyte, General Counsel and University Secretary		