

PART 1: GENERAL INFORMATION

Initiative title:	PIA 23-003 ClearDent
Department or program area:	Dental Hygiene
Initiative Sponsor (usually administrator overseeing implementation):	Sheldon Bailey
Initiative Lead name and title:	Jennifer Scott
Initiative Lead phone:	778-763-1114 ext 5607
Initiative Lead email:	scottj20@cnc.bc.ca
PIA Contributors (name, title and contact information)	Jennifer, Elyse, Miley
Privacy Officer:	Elyse Giddens
Privacy Officer phone:	250-562-2131 ext 5479
Privacy Officer email:	foipp@cnc.bc.ca

1.1. General information about the PIA:

<p>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.</p> <p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p>
<p>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.</p> <p><input type="checkbox"/> Yes <input checked="" type="checkbox"/> No</p>
<p>Related PIAs, if any:</p> <p>None</p>

1.2. What is the initiative?

The Dental Hygiene Program Coordinator is looking to implement a new software for patient records. The software name is ClearDent. It will house patient records.

This software would allow CNC to:

Securely access and manage dental records

Get the best of both a cloud and in-office solution.

Enhance productivity, patient communications, and patient care.

Move charts from paper to digital documents, thus increasing security and records management standards.

This was a recommendation outcome from the Dental Hygiene accreditation review. Dental Assisting program will also transition to the use of ClearDent.

1.3. What is the scope of the PIA?

The PIA is for the ClearDent software for the CNC's Dental Hygiene and Assisting programs.

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

Patient:

- first and last name
- Address
- Pronouns
- Birth date
- Cell phone number
- Home phone number
- Work phone number
- Email address
- Dentist name
- Dentist phone number
- Physician name
- Physician phone number
- Emergency contact name
- Emergency contact phone number
- Prescription for radiographs (which type of radiographs, how many, of which areas)
- Prescribed services such as local anesthetic with epinephrine, chlorhexidine use, scaling, prophylaxis, debridement
- Health history including medications
- Current level of illness (communicable disease risk assessment)
- Patient report: areas of concern and dental history

- Assessment of current radiographs and need for a radiograph prescription
- Tobacco assessment and willingness to quit
- Head and neck exam findings
- Odontogram findings (restorations, missing teeth, crowns, bridges, implants, etc)
- Caries risk assessment (includes past dental history, risk factors, preventative factors, disease indicators)
- Periodontal disease diagnostic statement
- Periodontal disease risk factors
- Periodontal assessment findings (probe depths, position of gingival margin, furcations, mobility, mucogingival involvement, clinical attachment loss)
- Image findings (radiographic findings)
- Deposit assessment
- Oral hygiene assessment
- Patient education
- Referrals
- Patient goals related to oral and general health
- Evaluation of care
- Evaluation of initial therapy

1.4. Did you list personal information in question 1.4?

Yes, [go to Part 2](#)

No, answer question 1.6 and submit Part 1 the Privacy Officer. You do not need to complete the rest of the PIA template.

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

Click or tap here to enter text.

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.

2.1 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: [REDACTED]	<input checked="" type="checkbox"/> Collection <input type="checkbox"/> Use <input type="checkbox"/> Disclosure	26.c.	Click or tap here to enter text.
Step 2: Student enters additional dental assessment data into ClearDent	<input checked="" type="checkbox"/> Collection <input type="checkbox"/> Use <input type="checkbox"/> Disclosure	26.c.	Click or tap here to enter text.
Step 3: Faculty review the information for accuracy	<input type="checkbox"/> Collection <input checked="" type="checkbox"/> Use <input type="checkbox"/> Disclosure	32.a., 32.b.	Click or tap here to enter text.
Step 4: Student references information to provide care to the patient	<input type="checkbox"/> Collection <input checked="" type="checkbox"/> Use <input type="checkbox"/> Disclosure	32.a., 32.b.	Click or tap here to enter text.
Step 5: Faculty reviews patient information to evaluate the student	<input type="checkbox"/> Collection <input checked="" type="checkbox"/> Use <input type="checkbox"/> Disclosure	32.a., 32.b.	Click or tap here to enter text.
Step 6: Patient services coordinator accesses patient records to initiate follow up, as needed	<input type="checkbox"/> Collection <input checked="" type="checkbox"/> Use <input type="checkbox"/> Disclosure	32.a., 32.b.	Click or tap here to enter text.
Step 7: Treatment letter outlines treatment performed and is sent to the patients' dentists	<input type="checkbox"/> Collection <input type="checkbox"/> Use <input checked="" type="checkbox"/> Disclosure	33.2.c	Click or tap here to enter text.

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
Step 8: Commission on Dental Accreditation of Canada reps review patient records during accreditation of dental programs	<input type="checkbox"/> Collection <input type="checkbox"/> Use <input checked="" type="checkbox"/> Disclosure	33.2.j.	Click or tap here to enter text.

Optional: Insert a drawing or flow diagram here or in an appendix if you think it will help to explain how each different part is connected.

Click or tap here to enter text.

2.2 Collection Notice

The information on this form is collected under the authority of section 26(c) of the Freedom of Information and Protection of Privacy Act. It is collected for the purpose of providing dental services, tracking patient records, accreditation and program review, and referring patients for dental care.

If you have any questions about the collection and use of your information, contact the College of New Caledonia School of Health Sciences healthsciences@cnc.bc.ca.

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.

3.1 Is any personal information stored outside of Canada?

- Yes
 No

3.2 Does your initiative involve sensitive personal information?

- Yes, go to [question 3.3](#)
 No, go to [question 3.4](#)

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

- Yes, go to [Part 4](#)
 No, go to [question 3.4](#)

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

██████████

15(1)(l)

- After you answer this question go to [Part 5](#).

PART 4: ASSESSMENT FOR DISCLOSURES OUTSIDE OF CANADA

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

4.1 Is the sensitive personal information stored by a service provider?

- Yes, fill in the table below (add more rows if necessary) and go to [question 4.3](#)
 No, go to [question 4.2](#)

Name of service provider	Name of cloud infrastructure and/or platform provider(s) (if applicable)	Where is the sensitive personal information stored (including backups)?
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	Click or tap here to enter text.

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

Click or tap here to enter text.

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

- No
 Yes
- If yes, describe the contractual measures related to your initiative.
Click or tap here to enter text.

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

Click or tap here to enter text.

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

Click or tap here to enter text.

4.6 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.

- This may include reference to the measures to protect the sensitive personal information (contractual, technical, security, administrative and/or policy measures) you outlined. Add new rows if necessary.

Privacy risk	Impact to individuals	Likelihood of unauthorized collection, use, disclosure or storage of the sensitive personal information	Level of privacy risk (consider 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, describe.
Click or tap here to enter text.	Click or tap here to enter text.	<input type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High	<input type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	<input type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High	<input type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High	Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.	<input type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High	<input type="checkbox"/> Low <input type="checkbox"/> Medium <input type="checkbox"/> High	Click or tap here to enter text.	Click or tap here to enter text.

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 4.6. 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.

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

No

Yes

- If yes, complete the Security Checklist below. This checklist will help determine whether you need a security assessment to ensure the initiative meets the reasonable security requirements of FOIPPA section 30. If a service provider or vendor is involved in the initiative, have them complete the "Third Party" section of Appendix A.

5.2 What physical security safeguards are in place to protect Personal Information in this initiative? Identify the elements of physical security that protect where the records for your initiative are stored (Check all that apply. Specify, "Other" if applicable)

Safeguard	At CNC	At Third Party
[REDACTED]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[REDACTED]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[REDACTED]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[REDACTED]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[REDACTED]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[REDACTED]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[REDACTED]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

15(1)(l)

What technical security safeguards are in place to protect Personal Information in this initiative? Describe the elements of technical security that protect where the records for your initiative are stored (e.g. secure passwords, encryption, firewalls, etc.)

Safeguard	At CNC	At Third Party
[REDACTED]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[REDACTED]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[REDACTED]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[REDACTED]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[REDACTED]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[REDACTED]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[REDACTED]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[REDACTED]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[REDACTED]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[REDACTED]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[REDACTED]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[REDACTED]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[REDACTED]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[REDACTED]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[REDACTED]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

15(1)(l)

What administrative safeguards are in place to protect Personal Information? Describe the elements of administrative security that protect where the records for your initiative are stored (e.g. aliasing, aggregation, policies/procedures, standards of practice, etc.)

Safeguard	At CNC	At Third Party
[REDACTED]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[REDACTED]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[REDACTED]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[REDACTED]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[REDACTED]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[REDACTED]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[REDACTED]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[REDACTED]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[REDACTED]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
[REDACTED]	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

15(1)(l)

5.3 Controlling and tracking access

Describe any additional strategies used to control and track access, if not indicated above.

Click or tap here to enter text.

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.

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

Patients enter health history information themselves

Students assess patients and the information collected is reviewed by faculty

Chart audit process and quality assurance checklists uses by students, which are then submitted to faculty for review and correction if required

6.2 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.

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

Yes

No

- Patient services coordinator can make changes as needed, and while the patient is in the clinic, they can request any changes as needed.
- Each time the patient is seen, the patient information is confirmed and updated as needed.

6.2.2 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?

Yes

No

N/A

6.2.3 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?

Yes

No

N/A

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

Yes, go to 6.4

No, go to Part 7

6.4 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

No

Patient records are retained for 16* years as per the Limitations Act.

Exemptions:

Records relating to minors must be retained for 16 years after the day the minor reaches the age of 19.

Records relating to persons under disability must be kept for 16 years after receiving formal notice that the person's disability has ended, or indefinitely.

PART 7: AGREEMENTS AND INFORMATION BANKS

Provide information about whether your initiative will involve an information sharing agreement, research agreement or personal information bank. If your initiative includes or will be part of a regular and systematic exchange of personal information with partners in or outside of government, you may require an [information sharing agreement \(ISA\)](#).

7.1 Does your initiative involve an information sharing agreement?

No

Yes

- If yes, complete the Information Sharing Agreement Supplement below and attach the ISA to this PIA.

Description of ISA: Click or tap here to enter text.
Name of main ministry or agency involved: Click or tap here to enter text.
Any other ministries, agencies, public bodies, or organizations involved: Click or tap here to enter text.
Business contact title and phone number for person responsible for maintaining the ISA: Click or tap here to enter text.
ISA start date: Click or tap here to enter text.
ISA end date: Click or tap here to enter text.

7.2 Will your initiative result in a personal information bank?

No

Yes

- If yes, complete the table below.

Describe the type of information in the bank: CNC Dental Programs Patient Records
Name of main organization involved: College of New Caledonia
Any other ministries, agencies, public bodies or organizations involved: N/A
Business contact title and phone number for person responsible for managing the PIB: Jennifer Scott scottj20@cnc.bc.ca

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.

8.1 Risk Response

Possible risk	Mitigation strategies
Caller imitates patient, or makes requests on someone else's behalf	Verification steps to confirm identity of patient. Use information release forms for consent to provide info to others.
Information on screen visible to those walking by the computer	Dental program staff and students will lock their computers when stepping away. Dental reception computer is tucked away from view.
Students or faculty could share patient information without consent	Student conduct policies in place Privacy protection policies and agreements for CNC employees Student are members of the Canadian Dental Hygienist Association and there is a Code of Ethics that applies Students complete professional practice courses that cover appropriate information use and disclosure
Emails about patients could be accessed by those outside of the dental program	Patients are referred to by chart number and personal information is left out of communication
Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.
Click or tap here to enter text.	Click or tap here to enter text.

PART 9: 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 department or program area will engage with their Privacy Office and if necessary, complete a PIA update.

Privacy Office Comments:

Dental programs to add privacy notice from section 2.2 to their digital and paper forms where patients provide their information.

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	Elyse Giddens	<i>Elyse Giddens</i>	June 15, 2023

Program Area Signatures

Role	Name	Electronic signature	Date signed
Initiative lead	Jennifer Scott		June 15, 2023
Initiative Sponsor Usually administrator overseeing implementation	Sheldon Bailey		June 15, 2023
IT Services Representative Only required if they have been involved in the PIA	Jordan Ingham		June 15, 2023

22(1)

22(1)

22(1)

APPENDIX A - Technical, Physical, and Administrative Safeguards

Technical, Physical, and Administrative Safeguards

This form helps to identify the physical, technical, and administrative safeguards in place that help protect personal information related to the initiative. If a third-party or vendor is involved in the initiative and will be responsible for the collection, use, storage, or disclosure of personal information, provide this form to them to complete.

Once completed, submit this form to foipp@cnc.bc.ca

Contact information:

Name:	[REDACTED]	Date:	5/30/2023
Role/title:	Product Manager		
Organization:	Prococious Technology Inc.		

22(3)(d)

Data storage location

Identify the location of the data storage related to the initiative (i.e. London, Ontario):
Where are you storing the personal information involved in your initiative?

Ans: [REDACTED]

15(1)(l)

Physical security safeguards

Identify the physical safeguards that protect where the records related to the initiative are stored (Check all that apply. Specify, "Other" if applicable)

Safeguard	Check all that apply
[REDACTED]	<input checked="" type="checkbox"/>

15(1)(l)

Technical security safeguards

Describe the elements of technical security that protect where the records for your initiative are stored (e.g. secure passwords, encryption, firewalls, etc.)

Safeguard	
[REDACTED]	■

15(1)(l)

Administrative safeguards

Describe the elements of administrative security that protect where the records for your initiative are stored (e.g. aliasing, aggregation, policies/procedures, standards of practice, etc.)

[REDACTED]	
[REDACTED]	<input checked="" type="checkbox"/>

15(1)(l)