HEAL Call-In Encounters Privacy Impact Assessment

Project Code	PC0765
Submission Date	October 15, 2018
Administrative Authority	[[As defined in Policy IM7800]] Director of Health Services – Rob Crisp
Author and Contact Information	Curtis Les, Senior Desktop Support Analyst, Desktop Support Services cles@uvic.ca
Reviewed By	
Review Date	[[Date of review – can be filled in by PMO or Reviewer]]

Purpose: The purpose of the Privacy Impact Assessment (PIA) is to assess risks associated with how a project plans to handle personal information. There are policy and legislative requirements and the purpose of the PIA is to ensure the project approach will be compliant with these requirements, and that any risks to privacy are mitigated or, if they cannot be completely mitigated, understood and accepted by the appropriate Administrative Authority as defined in section 2.00 of Policy IM7800:

> *Administrative Authority means individuals with administrative responsibility for units (e.g., Vice-Presidents, Chief Information Officer, Executive Directors, Deans, Chairs, Directors and other unit heads) and individuals with functional stewardship of university Information Resources.*

Roles:

The role of University Systems is to complete this document and provide guidance regarding security policy compliance and risks to the Administrative Authority.

The role of the Privacy Office is to review this document and provide guidance regarding privacy policy and legislative compliance and risks to the Administrative Authority.

The Administrative Authority is accountable for ensuring the Information Resource being implemented or changed as a result of this project is compliant with privacy and security policies and legislation and accepting risks associated with non-compliance on behalf of the institution.

1.0 Privacy Context

1.1 Description

[[Describe the project, the systems being implemented or changed as a result of this project, and what implications there are in terms of FIPPA.]]

Island Health requires tracking of patient calls to the shared after hours cell phone used by Health Services physicians. Regular reports with the statistics (not the details) of these calls need to be sent to Island Health. This project will create a secure and user friendly Connect (SharePoint) list for Health Services doctors to use for entering in some call details immediately after each call. This list can then be exported to generate a numbers only report for Island Health. When needed, the doctors can also select a checkbox to remind them to update patient charts in Accuro, Health Services Electronic Medical Records (EMR) application.

The data collected will be located with-in UVic's Sec. 15 - Disclosure harmful to law enforcement Sec. 15

1.2 Privacy Issues Related to this Project

[[Describe the privacy issues and how they are being addressed in the project approach.]]

The data being tracked are highly confidential health data for students. This includes:

1. The name of the doctor who took the call
2. The student's name
3. Student's date of birth
4. Student's phone number
5. The general reason for the call, with one of 6 options to choose from:
    a. Urgent medical concern
    b. Non-urgent medical concern
    c. Urgent PCMH concern (PCMH refers to Primary Care Mental Health)
    d. Non-urgent PCMH concern
    e. Prescription refill
    f. Other (common examples include clinic location or clinic hours)
6. Disposition of the call
    a. Telephone advice only
    b. Out of hours, in clinic visit (same day)
    c. Scheduled clinic visit (next day)
    d. Referral to another service
    e. Referral to walk-in clinic
    f. Referral to Emergency
    g. Other
7. Check boxes for whether a patient chart update is needed or a patient follow-up is needed.

Specific details of the health issue will not be included in the data collected.

The data in the Connect list will be extracted regularly, and a statistics report generated to be send to Island Health. The report will be given in person or sent by email. Private and personal information, including patient names and contact information will not be included in this report, only number of calls and disposition types. The data is deleted from the

Connect list after each annual report is completed, within 90 days of fiscal year end (June 30 each year). The longest possible retention period of the data is 15 months.

The doctors who log the calls may also refer to the call log to update patient charts, if they determine that is needed. The call log would assist with identifying the patient, but not with the actual health concern. These updates will be done directly in Accuro, the Health Services EMR application.

Read and write access to the HEAL On-Call Tracking Connect List will be controlled by Sec. 15 Sec. 15 Changes will only be made with approval of the Health Services Director.

1.3 Privacy Impact Assessment Scope

[[Describe what records will be under the possession or use of the institution or system and how the records will be managed to address FIPPA.]]

A record for each call will be kept in the On-Call Tracking Connect list. These records will be used to generate reports to be sent to Island Health. Records management practices will be applied to this data.

Project Scope	Privacy-Related Activities and Processes
Call in data records logging student calls to on-call doctors.	• Statistics reports generated based on the call log, and sent to Island Health. No PPI included in this report. • Call log can be referred to for finding the patient in Accuro for patient chart updates when doctor determines that is needed. • Data in the call log will be deleted annually by Health Services as a scheduled cleanup. This will occur no later than Sec. 15 with the longest possible data retention period being 15 months. • Statistics reports generated will be stored on Health Services secure Netdrive share as well as sent to Island Health. No PII will be included in the reports. • Access to the call log list will be restricted to the on-call doctors and Health Services personal only using security groups.

1.4 Related Privacy Impact Assessments

See Appendix A for SharePoint PIA classification tool done at SharePoint implementation.

1.5 Elements of Information or Data

Data	Description	Usage
Log of student calls to HEAL on-call cell phone	Doctor's first and last name, Student's first and last name, date of birth, phone number, general reason for the call (medical or PCMH concern, prescription, other), disposition of the call	• Used to generate regular reports for Island Health. • When required, will be referred to for updating patient charts in Accuro.

	(advice, scheduled visit, referrals), and check boxes for patient follow-up needed and patient chart required.	

2.0 Protection of Personal Information

2.1 Storage or Access outside of Canada

Storage – all data will be stored in Canada in the Sec. 15 **No data is stored outside of Canada.**

Access – data can be accessed outside of Canada by HEAL staff that have access, nothing prevents this as the Connect Service is accessible to the Internet for users that have access. In normal use cases, data would not be accessed from outside Canada.

2.2 Data-linking Initiative

In FOIPPA, "data linking" and "data-linking initiative" are strictly defined. Answer the following questions to determine whether your initiative qualifies as a "data-linking initiative" under the Act. If you answer "yes" to all 3 questions, your initiative may be a data linking initiative. If so, you will need to comply with specific requirements under the Act related to data-linking initiatives.	
Personal information from one database is linked or combined with personal information from another database;	No
The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	No
The data linking is occurring between either (1) two or more public bodies or (2) one or more public bodies and one or more agencies.	No. Data in Accuro and this new list are both owned by Health Services. Data sent to Island health includes no personal information.

2.3 Common or Integrated Program or Activity

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.	
This initiative involves a program or activity that provides a service (or services);	Yes – medical services to student patients.
Those services are provided through: **(a) a public body and at least one other public body or agency working collaboratively to provide that service; or** **(b) one public body working on behalf of one or more other public bodies or agencies;**	Yes. Health Services working on behalf and collaboratively with Island Health.
The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	Yes: Health Services contract with Island Health.

2.4 Personal Information Flow Diagram and/or Personal Information Flow Table

See diagram in Appendix B.

2.5 Risk Mitigation Table

[[Identify any privacy risks associated with the initiative and the mitigation strategy for each privacy risk. Consult the University Risk Likelihood and Impact scales to complete the Likelihood and Impact ratings for each risk.]]

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	*Lack of legal authority to collection, use or disclose PII*	Health Services has legal authority to collect and use PII. Disclosing of PII will not occur due to this project.	1	4
2.	*Unauthorized collection of PII by authorized individuals/processes/systems*	Form does not permit adding PPI information beyond Name, Date of Birth, and Phone Number, and predefined broad categories of call types and dispositions. There are no open text boxes for data entry.	1	4
3.	*Excessive collection of PII by authorized individuals/processes/systems*	Form does not permit adding PPI information beyond Name, Date of Birth, and Phone Number, and predefined broad categories of call types and dispositions. There are no open text boxes for data entry.	1	3
4.	*Inappropriate or unauthorized use of PII by authorized individuals/processes/systems*	Health Services policy prevents inappropriate or unauthorized use of PII.	1	4
5.	*Unauthorized disclosure by individuals/processes/systems*	Health Services policy prevents inappropriate or unauthorized use of PII.	1	4
6.	*Creation of new PII by data matching*	There is no connection between the SharePoint Call-in list and other systems.	1	4
7.	*Unauthorized tracking of individuals through transaction monitoring*	Health Services policy prevents unauthorized use of tracking individuals using this data	1	3
8.	*Data stored outside of Canada and in the public cloud*	Data would have to be deliberately copied outside of Canada for this to happen.	1	3
9.	*Data retention beyond prescribed timeline*	Data is regularly scheduled to be cleaned up (annually by Sec. 15 each year).	1	2
10.	*Risk of increased surveillance*	Surveillance is not a function of this project.	1	3

11.	*Unauthorized use as a records repository*	Data has a relatively short retention period of 15 months maximum, making it useless as a records repository.	1	2
12.	*Public perception*	No overly sensitive data will be collected, and only doctors and Health Services staff have access.	1	3
13.	*Use of existing PII data in a new system or business process*	All data added are new to the Call-In SharePoint list, there is no connection to existing data.	1	2
14.	*Risk of PII being gathered by unauthorized users*	The data is protected by Sec. 15 Sec. 15 as well as physical encryption on the Sec. 15 device commonly used to enter it. If the Sec. 15 were lost, it can be remotely wiped as an additional security measure.	1	4

3.0 Security of Personal Information

3.1 Please describe the physical security measures related to the initiative (if applicable).

The data reside on SharePoint servers located in the Sec. 15 Both data centres are strictly physically secured and locked down to access by Sec. 15 staff only.

3.2 Please describe the technical security measures related to the initiative (if applicable).

The data resides within Sec. 15 All storage and technical controls are managed by this service.

The primary means of adding data to the Connect list is using an on-call Sec. 15 This Sec. 15 is encrypted and locked with a passcode, which is enforced by University Systems ActiveSync policy. To access the Connect site, the users must also enter their Sec. 15 Access is limited to just those staff in HEAL that require it for their role in HEAL.

3.3 Does your department rely on security policies other than the Information Security Policy?

No.

3.4 Please describe any access control and/or ways in which you will limit or restrict unauthorized changes (such as additions or deletions) to personal information.

Only authorized users via Sec. 15 nested in Connect access groups will have access to read or modify the data. These users will be reviewed bi-annually and any changes made will be approved by the Director of Health Services.

3.5 Please describe how you track who has access to the personal information.

Membership of Sec. 15 will be regularly reviewed bi-annually and confirmed with the Director of Health Services as being correct. Removal of the membership to these groups will be added to the decommissioning process for Health Services.

4.0 Accuracy/Correction/Retention of Personal Information

4.1 How is an individual's information updated or corrected? If information is not updated or corrected (for physical, procedural or other reasons) please explain how it will be annotated? If personal information will be disclosed to others, how will the university notify them of the update, correction or annotation?

Authorized users of the Connect list can go and edit an entry directly as needed.

4.2 Does your initiative use personal information to make decisions that directly affect an individual(s)? If yes, please explain.

No

4.3 If you answered "yes" to question 4.2, please explain the efforts that will be made to ensure that the personal information is accurate and complete.

N/A

4.4 If you answered "yes" to question 4.2, do you have approved records retention and disposition schedule that will ensure that personal information is kept for at least one year after it is used in making a decision directly affecting an individual?

N/A

5.0 Further Information

5.1 Does this initiative involve systematic disclosures of personal information? If yes, please explain.

Yes. Regular reports of the data will be compiled and sent to Island Health. This is a requirement of Island Health from University Health Services. This data will only include statistical numbers, not the names, date of birth or phone numbers of patients.

Information Sharing Agreement – Required Information	
Description	***Health Services and Island Health Contract***
Primary department involved	***Health Services***
All other departments involved	***n/a***
Business contact title	***Valerie Kuehne, Vice-President Academic and Provost*** ***Gayle Gorrill, Vice-President Finance and Operations***
Business contact telephone number	***250-472-4925***
Indication of whether or not personal information is involved	***Yes. Only anonymized statistical information will be shared.***
Start date	***Annually renewed April 1st.***
End date (if applicable)	***March 31st, annually.***

5.2 Does the program involve access to personally identifiable information for research or statistical purposes? If yes, please explain.

No. The data is provided to Island Health for statistical purposes, but does not include any personal identifiable information.

5.3 Will a personal information bank (PIB) result from this initiative?

Yes. The maximum retention period of data is 15 months, with each years data deleted within 15 days of fiscal year end, by Sec. 15 annual.

5.0 Comments and Signatures

Chief Information Officer: Wency Lum

Comments:	
Date:	
Sign-Off:	

Administrative Authority: Rob Crisp

Comments:	
Date:	
Sign-Off:	

Portfolio Manager: [[Name]]

Project Comments:	
Date:	
Sign-Off:	

Consultation Checklist

IT Projects

The following leaders in each functional area can refer you to an appropriate subject matter expert to help develop the technical elements of your project plan and ensure it is complete.

Service Area	Impact? (Y/N)	Leader	Expert Consulted	Date of Consultation
Office of the CIO		Wency Lum		
Systems General Office		Chandra Beaveridge		
Client Technologies		Lance Grant		
Desktop Support Services	Y	David Street	David Street	Oct 12, 2017
Computer Help Desk		Marcus Greenshields		
Academic & Admin Services		Nav Bassi		
Client Account Managers		Garry Sagert		
Production and Technical Support		Rizwan Bashir		
Development Services		Scott Thompson		
Identity Services		Corey Scholefield		
UVic Online		Scott Thompson		
Data Centre Services		Kim Lewall		
Network Services		Jane Godfrey		
Infrastructure Services		Ron Kozsan		
Information Security Office	Y	Lance Grant		
Project Management Office	Y	Chandra Beaveridge		

Other Projects and Consultation

Department/Unit	Expert Consulted	Comments	Date of Consultation
Privacy Office			
Health Services	Kun Liu, Marianna Mazza, Rita Knodel		Nov 6, 2017

Revision History

Version	Date	Author	Comments
1.0	2017-09-26	Curtis Les	
1.1	2017-11-17	Curtis Les	Incorporated changes after initial review with David Street and Health Services.

Appendix A

PIA classification tool done for SharePoint governance and implementation (PC0391, PC0392). Date, January 2014.

Source:
https://connect.uvic.ca/sites/systems/PMO/_layouts/15/WopiFrame.aspx?sourcedoc=/sites/systems/PMO/repository/Completed%20Projects/PC0391-SharePoint%202013%20Governance%20Implementation/PC0391-SharePoint%202013%20Governance%20Implementation%20Project%20Plan.docx&action=default&DefaultItemOpen=1

Privacy Impact Assessment (PIA) Project Risk Classification Tool

Project Name:	SharePoint Technical Implementation
Project Code:	
Project Manager:	
Project Sponsor	

	IMPACT		Score
1	How many individual records will be stored, accessed or used?	50,000-100,000	4
2	What is the most sensitive type of Personal Information in these records?	Employee Information	7
3	Is any of the information owned by another organization?	No	2.5

	PROBABILITY		Score
4	Where will the information be stored?	Sec. 15 Sec. 15	1
5	How many users will have access to the information?	11-100	2
6	Will a third party (e.g. vendor or service provider) have access to the information?	No	2.5

PIA Priority Rating Table

Impact	Probability				
	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15	20	25

Colour Coding Key
LOW
MEDIUM
HIGH
VERY HIGH

Classification for this Project
8.3
HIGH

This tool is designed to assess the level of overall privacy and security risk associated with your project. It considers the volume and sensitivity of the information and how it is used. The overall risk is calculated as follows: RISK = IMPACT x PROBABILITY

Appendix B