PIA01515 — UBC Health Meeting of Experts

PART 1: GENERAL INFORMATION & OVERVIEW

1.1 Executive Summary

The UBC Health offers "Meeting of Experts," a longstanding initiative for patient engagement in health professional education coordinated by Patient & Community Partnership for Education (PCPE) in the Office of UBC Health. This allows active participation by "expert" patients and people with lived experience from the community as a way to train future health professionals. Patient educators contribute to the educational experience by sharing generalized life experiences relevant to healthcare training. The Health Mentors program is a longitudinal program for students from different health disciplines to learn from and with a mentor who has a chronic condition or disability, or is a caregiver. Groups (four students and a mentor) meet several times a semester, focusing on a specific health care topic at each meeting. Groups are self-directed with the mentor as the primary teacher. Students have a faculty supervisor from their professional program who reads the reflective journals written after each meeting. In addition, long-term research projects and studies are attached to the program.

Participation in the program is optional for students and requires registration, however, participation is graded). Individuals who wish to become patient educators are required to apply and submit significant personal information as part of this application process (see Data Elements). The Meeting of Experts web site (https://meetingofexperts.org) has been set up to make information collection easier.

1.2 Project Description

Meeting of Experts Website is a hub for patient and community involvement in health professional education at UBC. Originally developed as a virtual 'Community Centre for Health Professional Education' by PCPE in 2009 with funding from the UBC Teaching and Learning Enhancement Fund, the site was re-designed in 2019 in response to the UBC Health Patient Engagement Framework and recommendations to better support patient engagement in education across programs. UBC faculty and students can use the website to find the latest information about opportunities to learn from patients and connect with experienced patient educators. The platform facilitates community involvement in health professional education by providing a medium for interaction and engagement.

RISK CLASSIFICATION

The inherent privacy risk classification level of this PIA submission is 4 – **High**.
The residual risk classification level of this PIA submission at closure is 3 – **Medium**.

1.3 Scope

The scope of this PIA is the collection of personal information for the Meeting of Experts initiative by UBC faculty, staff and students, as authorized and outlined in this PIA.

1.4 Data Elements

Personal information collected from participants includes contact details, educational background, and any additional information voluntarily provided that is necessary for the program's objectives. Specific details such as dietary preferences and health conditions are collected only when explicitly relevant to the program activities and with explicit consent.

1.5 Storage or Access Outside of Canada (including back-ups and recovery)

Not applicable.

1.6 Data-Linking Initiative

This project is not considered a data linking initiative as contemplated under FIPPA s. (36).

1.7 Is this a Common or Integrated Program or Activity?

This project is not considered a common or integrated program or activity as defined in FIPPA Schedule 1.

PART 2: PROTECTION OF PERSONAL INFORMATION

2.1 Personal Information Flow Diagram/Table

Personal information is collected via secure web forms and managed through a controlled process ensuring data privacy and security at each step, from collection through storage to disposal. Access to the data is restricted to authorized personnel only, under strict security protocols.

2.2 Risk Mitigation Table

Privacy Risks					
Description	**Reference #**	**Inherent Likelihood**	**Inherent Impact**	**Response**	**Residual Risk**
Inadequate governance for personal information protection including policies and accountability	RK0020885	4 - High	4 - Major	Mitigate	3 - Medium
	Mitigation Plan: Appropriate mitigation strategies are in place to address any risks associated with personal information management, including rigorous access controls, data minimization, and regular audits of data usage and security measures.				
Over collection of personal information	RK0020845	4 - High	4 - Major	Mitigate	3 - Medium
	Mitigation Plan: Personal information collected will be strictly limited to what is necessary for managing participation in the program, as confirmed by the unit. The necessity and relevance of all data elements collected are regularly reviewed to ensure they align with the program's operational needs. The unit commits to enforcing data retention policies that comply with FIPPA standards. It is also recommended that the unit conduct a periodic review of access to other data repositories, such as UBC Student Information System and Workday Student, to avoid unnecessary data duplication and ensure compliance with privacy laws. This approach aims to reinforce data minimization and the principle of least privilege in data access.				
Retaining PI longer than necessary	RK0020847	4 - High	3 - Significant	Mitigate	3 - Medium
	Mitigation Plan: Indefinite retention of personal information is not authorized. Working with the UBC records Management Office, the unit has agreed to implement a blanket retention policy of seven (7) years for all data elements. Any personal information not required to be retained must be disposed in accordance with UBC Records Retention requirements. Development of a formal records retention plan is highly recommended.				
Inadequate controls for volume of personal information	RK0020848	4 - High	4 - Major	Mitigate	2 - Low
	Mitigation Plan: The unit has recognized the importance of securing personal information stored within UBC's on-premise shared drive folders. Access to this information is strictly limited to a small number of staff members, each authenticated through secure login protocols. Excel spreadsheets containing personal information will remain password-protected to prevent unauthorized access. Furthermore, the unit commits to routinely auditing and reviewing access permissions to these data repositories, ensuring that only individuals with a legitimate 'need-to-know' have access, in line with UBC's data governance policies and FIPPA requirements.				

2.3 Collection Notice

Registrants are required to click a check box indicating that they consent with data being stored according to the privacy guidelines (https://meetingofexperts.org/privacy-policy/). The full FIPPA collection statement appears only on the web site and not on the registration page.

2.4 Consent for Storage/Access Outside of Canada & Opt-Out Procedure (If Any)

All personal information is stored and accessed within Canada. In any case where data may need to be accessed from outside Canada, such as through international support services, explicit consent will be obtained from individuals, and data access will be conducted under strict supervision and for the minimum time necessary.

2.5 Consent Withheld Procedure

Not applicable.

PART 3: SECURITY OF PERSONAL INFORMATION

3.1 Physical Security Measures

This project is required to comply with UBC Policy SC14 (Information Systems Policy) and applicable UBC ISS (Information Security Standards).

3.2 Technical Security Measures

This project is required to comply with UBC Policy SC14 (Information Systems Policy) and applicable UBC ISS (Information Security Standards).

3.3 Security Policies, Procedures, and Standards

This project is required to comply with UBC Policy SC14 (Information Systems Policy) and applicable UBC ISS (Information Security Standards).

3.4 Tracking Access/Access Controls

Access to personal information within UBC is controlled through strict access protocols that ensure only authorized personnel have access. This includes employing industry-standard methods for secure authentication and role-based access.

PART 4: ACCURACY, CORRECTION, AND RETENTION

4.1 Updating and Correcting Personal Information

Not applicable.

4.2 Decisions That Directly Affect an Individual

This project captures personal information that directly affects an individual. Any data used to make a decision about an individual is required to be stored for a minimum of one year under s.(31) of FIPPA.

4.3 Records Retention and Disposal

This project is required to comply with UBC Records Management Policies. The UBC Records Management Office recommended a blanket retention policy of seven (7) years for deletion of data. The project also needs to be able to validate individuals who reapply after several years.

PART 5: FURTHER INFORMATION

5.1 Systematic Disclosures of Personal Information

This project does not involve the systemic disclosure of personal information.

5.2 Access for Research or Statistical Purposes

This project does not involve the disclosure of personal information for research or statistical purposes as contemplated under FIPPA s. (35).

5.3 Other Applicable Legislation and Regulations

This project is not subject to other applicable legislation or regulations.

PART 6: ACCESS AND PRIVACY MANAGER COMMENTS

6.1 Information or Materials Reviewed

Overall provided information was deemed reasonable to provide an understanding of operating privacy and security controls.

6.2 Analysis and Findings

The information provided for the review has established that the Meeting of Experts web site and the associated use-case, as presented by UBC Health, can be used in the proposed manner in compliance with FIPPA and UBC policies and standards.

The following are the key factors in that determination:

- Personal information is collected, stored, and accessed within Canada;
- Personal information is not disclosed to third parties external to authorized UBC staff members;
- Access to the data requires use of a valid login credentials with appropriate access authorities;
- Information is kept secure during transmission and at rest.

Accordingly, this initiative may proceed as proposed subject to the conditions outlines in the following section.

6.3 Conditions of Approval

None specified.

6.4 Review and Distribution

The Minister of Citizens' Services Direction 2-21, *Privacy Impact Assessment Directions* requires that all PIAs "designate the appropriate level of position that holds accountability for a PIA, proportionate to the sensitivity of the personal information and/or the risks of the initiative" (s. D8).

Accountability is maintained by the role or position, regardless of who fills the role.

Under UBC Policy SC14, Administrative Heads of Unit are responsible for:

- ensuring that UBC Electronic Information and Systems are secured with adequate controls, with particular care concerning User identification and validation measures;
- ensuring, as appropriate or required, that UBC Electronic Information within their area of responsibility is maintained, transmitted, and stored in a secure and consistent manner that adheres to all relevant University policies and standards;
- authorizing access for individuals to UBC Electronic Information and Systems within their area of responsibility;
- renewing, retiring, and revoking User authorizations within their area of responsibility.

Holding accountability for the privacy risks of this initiative includes:

- reviewing the mitigation strategies listed in the relevant risk tables and ensuring those strategies are maintained throughout the life of the initiative;
- ensuring accountability is transferred to any individual who assumes this role;
- if there are any changes to the initiative, including to the way personal information is collected, used, stored or disclosed, ensuring the PIA team is engaged, and if necessary, completing a PIA update; and
- understanding what your privacy obligations are, and if not, following up with the PIA team.

Assessment Acceptance
Catherine Kline

Distribution
Requestor: Catherine Kline, Research Coordinator **Project Manager**: Catherine Kline, Research Coordinator **Owner**: Catherine Kline, Research Coordinator **Risk Advisor**: Christian Stockman, Information Security Risk Advisor

PIA Request Submission	Report Completion
2020-06-02	2021-09-17