Privacy Impact Assessment: Zoom Video Communications Platform

Name of Organization	BCNET		
PIA Drafter:	Hooper Access and Privacy Consulting Ltd.		
Email:	bev@hooperconsulting.ca tjreid@hooperconsulting.ca	Tel:	250 896-4272 250 388-0145
Program Manager:	Dean Crawford - Director Shared Systems and Technology		
Email:	dean.crawford@bc.net	Tel:	250 721-8477 250 418-0593

1. Description of the Initiative

BCNET is taking the lead on the development of this Privacy Impact Assessment (PIA) for the Zoom platform, on behalf of its members and affiliations.

BCNET is a federally incorporated not-for profit services and information technology organization that represents the interests of its member institutions comprised of 25 publicly funded universities, colleges, institutes, and research organizations across British Columbia. It represents all public, post-secondary education institutions in the province and provides shared services to its members in the areas of networks, procurements, licensing, and IT services.

This unique, collaborative shared services model provides a multitude of benefits to its members from reducing and containing costs and increasing spending power, to decreasing duplication and improving service quality and productivity. The model cultivates a strong community, where members actively engage with peers to share, explore, and develop innovative ideas and solutions as they tackle a broad spectrum of common and unique research and education technology challenges and topics. BCNET strives to add value to its membership by leveraging an advanced network that provides economies of scale to maximize efficiencies and drive down collective costs, while at the same time, continuing to facilitate collaborative innovative solutions that meet the needs of their stakeholders in support of world-class research and education.

It is the intent of this PIA to determine privacy risks associated with the implementation of the Zoom platform to support remote business, learning and administrative uses.

Zoom video communications provides remote conferencing services using a cloud-based Software as a Service (SaaS) platform (e.g. online meetings across different locations, online teaching/courses, virtual classrooms, distance learning – content/lessons, group project collaboration, etc.). Sessions can be enabled for both desktop and mobile applications and users are provided with the option to activate a webcam or microphone (sessions can also be potentially recorded by the meeting host). BCNET has selected Zoom's AWS Canada tenant as its data centre and is following Zoom's best practice settings for its account. All video conferencing is encrypted with password protection, but without imposition of a waiting room or disallowing non-host screen sharing across all accounts. Meetings taking place through the BCNET's Zoom Canada architecture are identified with the Canadian URL of "https://ca01web.zoom.us".

The following Zoom functionality is not available/supported in the Canadian instance:

- Full global cluster redundancy and resiliency global cluster redundancy and resiliency (Zoom's #1 architecture priority is focusing on making the Canadian cluster more robust)
- Zoom Phone
- Conference Room Connector (traditional H.323/SIP video endpoint) data isolation
- Marketplace/API
- Large Webinar capacity (10,000+)

Zoom is headquartered in San Jose, California and uses cloud-based data centres around the world (including the Canadian offering), which BCNET has selected. Zoom is a proven content sharing platform, has established experience offering online conferencing tools and is actively used by many Canadian universities.

A key component of facilitating innovative information technology (IT) solutions through BCNET is ensuring they are hosted, accessed, managed and protected within a secure environment in accordance with Provincial *Freedom of Information and Protection of Privacy Act* (FIPPA), privacy laws, regulations and controls.

BCNET is dedicated to ensuring that the use of the Zoom system meets provincial privacy and security legislative requirements, policies and practices, and strives to reduce the privacy risks associated with the legislative requirements accordingly. These privacy risks are managed through a combination of technical, administrative and physical controls that mitigate the associated risk. This privacy impact assessment (PIA) is intended to support the utilization of

Zoom by BCNET and its members to ensure that this service is offered and provided in a way that is compliant with the FIPPA.

2. Scope of this PIA

This PIA has been developed with a focus on the privacy protection and security measures deployed by the Zoom video conferencing platform in its standard configuration.

3. Related Privacy Impact Assessments

No other PIA's have been completed on this initiative by BCNET. A related PIA on BCNET - Amazon Web Services (AWS) Canada has been completed.

4. Elements of Information or Data

The collection of all personal information from the individual will continue to be the responsibility of the BCNET member (e.g. the provincial, public sector organization managing the application). Use and disclosure of that personal information may occur while utilizing the Zoom platform in order to deliver BCNET member programs and services and meet operational requirements.

In this context, personal information (PI) required from BCNET members to participate in the Zoom environment includes:

- Participant name
- Participant personal email
- Participant personal ID/Acct username
- Participant personal tel/mobile telephone number
- Participant physical address (if connecting from an offsite location)
- Status: Status information as to whether a participant is active, out or busy (user enabled)
- Participant personal IP address
- Recording Feature: audio/video/screen sharing content, operating system type and version, client version, IP addresses along the network path and the MAC address of the user's internet connection
- Content: Files and file name, sizes and types, whiteboard content, snapshots and background images
- Usage of the Service: actions taken, date and time, frequency, duration, quantity, quality, network connectivity, and performance information related to logins, clicks, messages, contacts, content shared, calls, use of video and screen sharing, meetings, cloud recording, and other feature usage information
- User generated information: Meeting title, invitation content, participants, meeting link, date, time and duration, activity recorded in the meeting (such as joining or leaving), third-party integrations with the date, time, person engaged in the activity, and other participants in the meeting with the date, time, duration
- Messages: Message content, sender and recipients, date, time, and read receipts

- Geolocation: Location of user for optimization and connection to data centre and to support compliance (users can opt in/out)
- Cookies and tracking: Browser type, Internet service provide (ISP), referring/exit pages, files viewed, operating system, date/time stamp (users can opt in/out)

5. Storage or Access outside Canada

BCNET will be using the Zoom AWS Canada instance and Canadian region (data in transit and at rest). Assessment of this platform, including disaster recovery options, is outlined in the BCNET Amazon Web Services (AWS) Canada Privacy Impact Assessment. Information will not be stored or accessed outside of Canada.

The BCNET accounts use anonymous userid's and BCNET email addresses stored in the BCNET Active Directory (AD). Mail forwarding occurs at the BCNET on-premise AD to individual member user accounts. In this setup, username and email remain anonymous to Zoom and Name, Telephone Number and Physical Address would only be available to Zoom support staff if entered by the individual user.

Zoom has provided a configuration which stores data on servers exclusively located in Canada that can anonymize users. BCNET is utilizing this service and all recordings and chat logs reman in Canada. Additionally, meetings are aggregated into a single stream in either Vancouver or Toronto.

Zoom provides users with control over data by leveraging a network that routes traffic through a real-time meeting zone that provides the best performance. Users cannot change or opt out of their default region (Canada), which is locked and where the related account is provisioned.

Information discussed by the participants during conferencing sessions flows through Zoom servers and is collected if the recording feature (audio/video/chat logs) has been enabled. If the meeting host activates the local recording option, the recordings will be stored on the host's computer. All participants will receive an automatic notification of a red flashing light on the meeting screen and an audio cue when recording is enabled.

6. 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 and you must comply with specific requirements under the Act related to data-linking initiatives.	
1. Personal information from one database is linked or combined with personal information from another database;	No

2. The purpose for the linkage is different from those for which the personal information in each database was originally obtained or compiled;	N/A
3. 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.	N/A
If you have answered "yes" to all three questions, please contact your privacy office(r) to discuss the requirements of a data-linking initiative.	

7. 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.	
1. This initiative involves a program or activity that provides a service (or services);	Yes
2. 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
3. The common or integrated program/activity is confirmed by written documentation that meets the requirements set out in the FOIPP regulation.	No
Please check this box if this program involves a common or integrated program or activity based on your answers to the three questions above.	

8. Personal Information Flow Diagram and/or Personal Information Flow Table

Personal information is collected by Zoom for the purpose of registering accounts, operating video sessions, responding to requests, improving the service, technical support, providing updates, sharing users' identity with other users on the platform and complying with legal or contractual obligations. Personal information may also be accessed, collected and used to facilitate interactions between students, staff and educators for the purposes of collaboration on an operational or educational project.

This table addresses the flow of personal information while using the Zoom video conferencing system (e.g. BCNET members - students, instructors, employees).

Personal Information Flow Table – Users			
	Description/Purpose	**Type**	**FOIPPA Authority**
1.	User is registered for system by BCNET staff using a BCNET email account. The BCNET staff sets email forwarding from this account to the correct institutional contact. Zoom has a process for records retention to ensure that Personal Information is retained for no longer than necessary to fulfill the obligations or meet legal retention requirements. Zoom retains account information only for as long as necessary to comply with legal obligations (e.g., tax compliance) but no longer than 10 years after account termination. Customer content is retained for the life of the account; however, customers are free to delete this content at anytime. When an account is terminated, customer content is deleted after 60 days or as agreed with you in a separate contract. Account information is information provided to Zoom when a user or company signs up for the Service. Customer content is information provided by the customer to Zoom through the usage of the service. Customer content includes cloud recordings and instant messages.	Collection	*Section 26*
2.	Zoom uses personal information to register users and enable ongoing service.	Use	*Section 32*
3.	User (meeting host) sends invitations to participants to join Zoom session.	Use	*Section 32*
4.	User accepts invitation and securely logs into Zoom to attend video conference (discussion may include personal information).	Use	*Section 32*
5.	User engages in meetings and uses service (which may or may not be recorded by the meeting host). Metadata about session connections is temporarily stored on Zoom servers for meeting aggregation purpose. Recording and chat logs will be stored until removed by the meeting host on Canadian servers.	Collection	*Section 26*
6.	If unrecorded, data flows through Zoom server without being stored. Data elements stored and/or processed by Zoom platform	Use	*Section 32*

	are as follows: -Customer Account Information: Company Name, Customer Account Owner Contact Information (Name, Email, Phone), Customer Business Contact Information (Name, Email, Phone), Business Address, Customer Account Type, Customer Account Plan, Scheduled Meetings -User Profile: First Name, Last Name, Phone (optional), Email, Password (if SSO is not used), Profile Picture (optional), Department (optional) -Meeting Metadata: Topic, Description (Optional), Participant IP Addresses, Device/Hardware Information, Meeting Statistics/Metrics, Start Time, Join Time, Leave Time IM chat logs and metadata (in-meeting chat, persistent chat--if enabled by the customer) If enabled, Zoom's in-meeting file transfer* allows customers to send files to other meeting participants during the meeting through the in-meeting chat. Cloud Recordings* (if enabled by the customer): MP4 of all video, audio and presentations, M4A of all Audio, Text file of all in meeting chats, Audio transcript file. Cloud recordings can be stored in the Zoom platform (AWS S3 storage) or the recording can be re-directed and stored locally by the customer. *Please refer to https://support.zoom.us/hc/en-us/articles/203741855-Cloud-Recording for more information*		
7.	Zoom discloses personal information to third parties and affiliated companies (e.g. data processing, storage, to provide services and support, etc). Zoom can only access PI permitted outside of Canada only if the members themselves enter their name, phone number or address.	Disclosure	*Section 33*

9. Risk Mitigation Table

It should be noted that primary responsibility for the management and administration of any physical and/or technical security risks is born by BCNET members choosing to deploy and utilize Zoom. These privacy risks are managed through a combination of technical, administrative, and physical controls that are designed and in place to mitigate each associated risk.

For related information regarding the AWS platform, please refer to the Amazon Web Services Canada Privacy Impact Assessment previously completed by BCNET.

Risk Mitigation Table				
	Risk	**Mitigation Strategy**	**Likelihood**	**Impact**
1.	Unauthorized individuals at BCNET could access the personal information and use or disclose it for personal purposes (within the BCNET member environment).	Employee Code of conduct and Non-disclosure agreements; Use of Information & Technology Policies, password protected access, user access to system, based on need to know basis, permission restrictions, controls, and monitoring.	Low	High
2.	BCNET member personal information data is compromised during transmission from the member to Zoom.	Zoom has acceptable security controls in place. It uses end to end encryption and BCNET administrators will ensure that identified vulnerabilities have been patched. Also, if users turn off the record feature, no sensitive or personal information will be collected and stored. Data transmitted to Zoom is encrypted using TLS 1.2 protocol and cloud recordings are protected in transit and at rest using AWS Server-Side encryption. Zoom Client (application): Data In-Transit: By default, Zoom encrypts in-meeting and in-webinar presentation content at the application layer using TLS 1.2 with Advanced Encryption Standard (AES) 256-bit algorithm. • For dial-in participants joining by phone, the audio is encrypted until it leaves Zoom's data centers and is transferred	Low	High

		to the participant's phone network. • Encryption can be required for H.323 and SIP devices joining Zoom meetings. This setting is configured at the account level, group, or user level. Once enabled, encryption will need to be enabled on these devices when joining your Zoom meeting or they will receive an error and be unable to join. **Note:** You can also enable or disable encryption for chat. For more details, please refer to the article: https://support.zoom.us/hc/en-us/articles/201362723-Encryption-for-Meetings Additionally, Zoom supports secure voice calls across all supported SIP devices, desktop, and mobile clients. Zoom Phone supports standards-based encryption using SIP over TLS 1.2 Advanced Encryption Standard (AES) 256-bit algorithm for calls and during phone provisioning sessions. In addition, call media is transported and protected by SRTP with AES-256 bit algorithm for Zoom desktop and mobile clients, and with AES-128 bit algorithm for devices. Data At-Rest: Data at rest is protected leveraging Amazon Server Side Encryption (SSE) using 256-bit Advanced Encryption Standard (AES-256).		

		Note: Zoom 5.0 supports AES-256 ECB and also supports AES-256 GCM encryption. A system-wide account enablement to GCM encryption will occur on May 30, 2020, and only Zoom clients on version 5.0 or later, including Zoom Rooms, will be able to join Zoom Meetings starting May 30.		
3.	Zoom Security Breach	Zoom breach protocols are in place to reduce risks to member data in the event of a security breach. Furthermore, data is always encrypted during transmission or while being stored by Zoom.		
4.	User account is accessed externally by another individual	Unique login/password established by end user and enforced by BCNET member institution.	Low	High
5.	Inherent risks in providing access to third party (Zoom)	All Zoom employees are required to abide by BCNET's privacy obligations via the contract & privacy protection schedule, including BCNET policies and guidelines (e.g. IT & FIPPA).	Low	Medium
6.	Users are not appropriately authenticated for specific Zoom sessions	Access to sessions is via emailed invitation. However, any recipient can email the invitation to others without limitation. Restricting the sensitivity of recorded information, limits this risk.	Low	High
7.	Zoom may provide personal information to third parties	Zoom uses Service Agreements and Data Processing Agreements as contractual controls established to ensure that personal information collected, transmitted, processed, stored or disclosed to or retained by third parties is limited to defined parameters for access, use and disclosure.	High	Med

		Participants can mitigate this risk by using a non-identifying name and by using privacy browser extensions to prevent third-party tracking and access to their information.		

10. Collection Notice

Each BCNET member is responsible for ensuring the appropriate collection notification (for the specific application/program) is in place prior to the collection of personal information and before transmission to the Zoom Server. Zoom software allows for the recording of sessions which should be reflected in the notification statement.

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

BCNET and third-party service providers are responsible for ensuring the physical security of all data while in their custody and/or control (including data at rest or in transit) and must meet applicable physical security standards required by their organization.

AWS:

For related information regarding the AWS platform, please refer to the Amazon Web Services Canada Privacy Impact Assessment previously completed by BCNET.

Zoom:

Zoom uses Amazon Web Services (AWS) to host web services and cloud infrastructure and data centre providers to host its real-time communication services. This includes computing power, storage and other application services delivered over the Internet. AWS and the data centre providers are responsible for the physical security and environmental controls within these data centre.

Zoom indicates that the existence and operation of controls at AWS and the data centre providers are verified by Zoom's security team on an annual basis through review of external service auditor reports. Any exceptions noted in the review are investigated with the service providers and reported to Management.

Zoom has a formal Physical and Environmental policy in place. Physical access to our office facilities is protected by 24x7 camera surveillance, keycode/RFID access, staffed reception, and provided security staff. Additionally, Zoom leverages the physical and environmental protection of its Tier 3 and above data center providers. Only authorized personnel have access to our datacenters.

In the data centers, physical access is controlled by access list, badge, mantrap, guards,

perimeter fencing, CCTV, and biometrics. All visitors must be escorted by authorized Zoom personnel at all times. The data centers uphold the necessary safety requirements for fire protection and utilize solid building construction to safeguard assets.

Zoom's co-location facilities are N+1 and have environmental controls such as:
- Temperature and Humidity Controls
- Power systems that are fully redundant and scaled to accommodate component failure.
- Has resilient emergency lighting in place
- Emergency Lighting
- Fire Protection
- Water Damage Protection

For Amazon AWS environment, Zoom leverages AWS physical security safeguards.

Physical access controls for data centre include key cards and biometric scanners, perimeter and interior IP-DVR, in-house staffing and mantrap and perimeter fencing. Access reviews are performed quarterly for physical access to the collocated data centres.

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

BCNET members and third-party service providers are responsible for ensuring the technical security of all data in their custody and/or control (including data at rest or in transit) and must meet applicable technical security standards required by their organization. Members are solely accountable for Security Risk Assessments for their respective organization.

AWS:

For related information regarding the AWS platform, please refer to the Amazon Web Services Canada Privacy Impact Assessment previously completed by BCNET.

Zoom:

Zoom uses a combination of industry-standard security technologies, procedures, and organizational measures to help protect users' Personal Data from unauthorized access, use or disclosure. When users' personal information is transferred over the Internet, Zoom protects it using Secure Sockets Layer (SSL) encryption technology. This includes:

- Submission of privacy practices to independent assessment and certification with Trust Arc
- Annual SSAE-16 SOC 2 audit by a qualified independent third-party
- Regular vulnerability scans and penetration tests to identify new threats
- Execution of "Data Protection Agreements" for adequate transfer mechanisms
- Protection of data in transit by TLS 1.2 using 256-bit Advanced Encryption Standard (AES-256)
- Leveraging the physical and environmental protection of TIER 1 data center providers
- Hosting facilities with 24/7 manned security and monitoring
- Limiting retainment of accounts to 30 days after termination to assist with product reactivation upon request. After 30 days, the account is permanently deleted

Zoom has a formal Incident Management Policy that addresses incident handling, escalation, and communication. All incidents are reported through Zoom's ticketing system, Zendesk. Zoom posts any general incident announcement and other announcements including scheduled maintenance, outages, and updates through at their status page which can be found at status. Zoom.us.

For incidents affecting a specific user, Zoom will notify the account owner and administrator(s) through email or as specified in the fully executed service agreement. Access to Zoom's platform (the "system") requires a unique identification ("ID") to establish accountability with user logins. Administrator access is restricted to authorized system and security administrators. New user access to production is granted in accordance with the role matrix defined in the access control policy. Additional access requires management approval. Access to critical systems and applications requires user IDs with passwords or public key authentication. Zoom does not monitor, view, or track the video or audio content of meetings (or webinars) or share customer data with third parties.

13. Does your branch/department rely on any security policies?

BCNET members and third-party service providers are responsible for the deployment, dissemination and administration of organizational security policies as it relates to the management of personal information in their custody and/or control.

AWS:

For related information regarding the AWS platform, please refer to the Amazon Web Services Canada Privacy Impact Assessment previously completed by BCNET.

Zoom:

Zoom has implemented safeguards to protect users' privacy, which includes robust and validated controls to prevent unauthorized access to any content that users share during meetings, including – but not limited to – the video, audio, and chat content of those meetings. Unless a meeting is recorded by the host, the video, audio, and chat content is not stored. Participants are notified through both audio and video when the host is recording a meeting through Zoom and have the choice to opt in or leave the meeting. When the meeting is recorded, it is, at the host's choice, stored either locally on the host's machine or in the Zoom cloud. Zoom has access controls to prevent unauthorized access to meeting recordings saved to their cloud. Zoom does not mine user data or sell user data of any kind to anyone.

https://zoom.us/privacy https://blog.zoom.us/wordpress/2020/03/29/zoom-privacy-policy/

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

BCNET members and third-party service providers are responsible for the strict management and administration of user access based on a "need to know" principles including maintenance and enforcement.

AWS:

For related information regarding the AWS platform, please refer to the Amazon Web Services Canada Privacy Impact Assessment previously completed by BCNET.

Zoom:

Zoom has a formal Access Control Policy in place and administrative, physical, and technical safeguards and processes in place that prevent unauthorized access to the production environment. Only authorized operation personnel are allowed access. Access is role-based and least privileged. Quarterly access reviews are conducted to ensure that access is appropriate to the role. Zoom also has detailed job descriptions for technology/security roles based on appropriate access level and job function.

Administrator access is restricted to authorized system and security administrators. New user access to production is granted in accordance with the role matrix defined in the access control policy. Additional access requires management approval. Access to critical systems and applications requires user IDs with passwords or public key authentication.

Zoom employees will not actively monitor any customer sessions unless requested by the BCNET member for support (install, implement, maintain, repair) or trouble-shooting purposes. No data is stored (e.g. login, metadata). Being a cloud-based service, most of the support solutions will be leveraging from the information and tools provided by Zoom.

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

BCNET members and third-party service providers are responsible for ensuring that access to all personal information in their custody and/or control is secure, monitored and reviewed/audited on a regular basis.

AWS:

For related information regarding the AWS platform, please refer to the Amazon Web Services Canada Privacy Impact Assessment previously completed by BCNET.

Zoom:

Zoom offers customers dashboard, usage reporting and operational logs which can be accessed by account owner and designated administrator within the account management page. Zoom also collects various system and monitoring and audit logs that are maintained and reviewed by its Operations team. Systems logs are not available for external consumption.

Administrator access is restricted to authorized system and security administrators. New user access to production is granted in accordance with the role matrix defined in the access control policy. Additional access requires management approval. Access to critical systems and applications requires user IDs with passwords or public key authentication.

Zoom, its third-party service providers, and advertising partners (e.g., Google Ads and Google Analytics) automatically collect some information about users when using Zoom (methods such as cookies and tracking technologies). Information automatically collected includes Internet protocol (IP) addresses, browser type, Internet service provider (ISP), referrer URL, exit pages, the files viewed on the Zoom site (e.g., HTML pages, graphics, etc.), operating system, date/time stamp, and/or clickstream data. Zoom's Privacy Policy states that it uses this information to offer and improve services, trouble shoot, and to improve its marketing efforts. While the disclosed data is not linked to a username, it is potentially re-identifiable through the mosaic effect.

16. **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 public body notify them of the update, correction or annotation?**

Updates to an individual's information (e.g. student, employee) is annotated in Zoom by the BCNET member. The BCNET member or individual will then contact each area to make notification of the change.

AWS:

For related information regarding the AWS platform, please refer to the Amazon Web Services Canada Privacy Impact Assessment previously completed by BCNET.

Zoom:

Zoom users can update their personal data from the Account Profile page at any time. Requests to access update or remove personal information from Zoom's storage, can be sent by email to privacy@zoom.us or by mail to the following address:

Zoom Video Communications, Inc.
Attention: Data Privacy Officer
55 Almaden Boulevard, Suite 600
San Jose, CA 95113

Zoom does not offer functionality to update or annotate personal information stored on AWS? servers (meeting recordings).

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

Yes. To provide a video communications tool used by BCNET members for operational purposes and to provide services. Use of Zoom may contain content which includes personal information.

18. **If you answered "yes" to question 17, please explain the efforts that will be made to ensure that the personal information is accurate and complete.**

Responsibility for ensuring all personal information is up to date and accurate lies with the registered BCNET member user (e.g. student, instructor, employee).

19. If you answered "yes" to question 17, do you have a records retention and/or 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?

Each BCNET member is responsible for respective records retention and/or disposition schedules specific to their organization.

20. Does the initiative involve systematic disclosures of personal information? If yes, please explain.

No.

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

No.

22. Will a personal information bank (PIB) result from this initiative? If yes, please list the legislatively required descriptors listed in section 69 (6) of FOIPPA. Under this same section, this information is required to be published in a public directory.

Yes. BCNET members will be creating PIB's as result of using Zoom.

Signed on Behalf of BCNET:

Dean Crawford — 22 September, 2020

Dean Crawford
Director, Shared Systems & Technology
BCNET

Date

Bala Kathiresan
Bala Kathiresan (Oct 13, 2020 18:24 EDT)

Oct 13, 2020

Bala Kathiresan
President & Chief Executive Officer
BCNET

Date

A final copy of this PIA (with all signatures) must be kept on record.

2020 10 Zoom PIA

Final Audit Report 2020-10-13

Created:	2020-10-13
By:	Heidi Vien (heidi.vien@bc.net)
Status:	Signed
Transaction ID:	CBJCHBCAABAAmi0fPX0Pny_2vyM5-YTaGstVi2_5zUWK

"2020 10 Zoom PIA" History

Document created by Heidi Vien (heidi.vien@bc.net)
2020-10-13 - 10:05:33 PM GMT- IP address: 69.172.172.89

Document emailed to Bala Kathiresan (bala.kathiresan@bc.net) for signature
2020-10-13 - 10:07:01 PM GMT

Email viewed by Bala Kathiresan (bala.kathiresan@bc.net)
2020-10-13 - 10:23:24 PM GMT- IP address: 70.49.151.248

Document e-signed by Bala Kathiresan (bala.kathiresan@bc.net)
Signature Date: 2020-10-13 - 10:24:01 PM GMT - Time Source: server- IP address: 70.49.151.248

Agreement completed.
2020-10-13 - 10:24:01 PM GMT