North York Rehabilitation Centre Corp
Suite 1385 – 1095 West Pender Street
Vancouver, BC V6E 2M6
Phone: (778) 372-1410
Fax: (778) 372-1411

SECURE VIRTUAL IME SERVICES THROUGH ZOOM - NYRC

NYRC is dedicated to providing the most innovative and secure IME services in Canada. In response to the COVID-19 Pandemic NYRC has developed a host of Virtual IME services for our clients and assessors, and one of the virtual platforms NYRC is utilizing to deliver these services is Zoom.

Although Zoom is compliant with Canadian Data Protection regulations, including the Personal Information Protection and Electronic Documents Act (PIPEDA) and, locally, the Personal Health Information Protection Act (PHIPA), there have been some concerns raised about the platform's security and whether Zoom is safe to use for meetings that discuss private information.

The security issues that are being raised in the news were due to a Zoom user setting error and not due to inherent security or compliance issues with Zoom itself. What is being coined "**Zoom-bombing**" occurs when the platform is used incorrectly or irresponsibly. **Zoom-bombing** occurs when an uninvited party gains access to a virtual meeting and disrupts the integrity and security of a virtual call. This typically occurs when a 9-digit Zoom meeting ID is shared publicly (i.e. via social media, insecure email, etc.). Industry professionals have provided the below suggestions to prevent such breaches, all of which NYRC follows:

1) **Never share a meeting ID publicly:** 9-digit Zoom meeting IDs should be sent to only those who are invited to attend the virtual meeting.
2) **Do not use your Zoom account's Personal Meeting ID for all meetings:** Rather, when scheduling a meeting, generate a random meeting ID in the Zoom option panel to ensure that you have a unique meeting ID for each and every call.
3) **Enable password protection to access meetings:** Ensure that when scheduling a meeting you enable the password setting. This ensures that only parties with the meeting password and invite can access the call.
4) **Enable the virtual waiting room:** Hosts can ensure that a virtual waiting room is enabled for meetings on a case-by-case basis or by making it a default for all meetings. The virtual waiting room enables the host to restrict meeting access to invited guests only. When trying to join a meeting, invitees are put on hold in the virtual waiting room and must be given specific approval by the host to join. If an uninvited guest tries to join the call, the host would be notified and would deny access accordingly.

Along with the above recommendations, NYRC has taken the following additional steps to protect the integrity of its virtual meetings:

1) **NYRC is the "Host" of all virtual meetings:** This not only ensures that NYRC has complete control over the settings and execution of the virtual meeting, but also ensures that NYRC is able to confirm the identity of the invitees before admitting them to the virtual meeting.
2) **NYRC restricts screen sharing:** NYRC does not allow any party to share their screen with other meeting attendees and reserve the screen sharing capability for the Host only.

North York Rehabilitation Centre Corp
Suite 1385 – 1095 West Pender Street
Vancouver, BC V6E 2M6
Phone: (778) 372-1410
Fax: (778) 372-1411

3) **NYRC "Locks" meetings that are in progress:** Once NYRC has confirmed that all parties are connected and only those invited are within the virtual meeting, NYRC is able to lock the meeting within the Zoom platform. This ensures that no other party, even if they have a meeting ID, a password or otherwise can join the meeting in progress.
4) **NYRC disables meeting recording capabilities:** NYRC does not allow the recording of any of its medical assessment services, including its virtual assessments. Zoom recording is disabled for all NYRC Virtual IMEs, making the recording of assessment via the Zoom platform impossible.
5) **NYRC disables the "Chat" function within zoom**: The chat function within Zoom allows meeting attendees to message each other during the virtual meeting, including the ability to share documents. NYRC disables this function to ensure that no documentation can be shared through the Virtual Network.
6) **NYRC is a Licensed User of Zoom:** For licensed professional account holders such as NYRC, Zoom comes with further security protections and is completely compliant with Federal and Provincial Privacy regulations including PIPEDA/PHIPA.
7) **NYRC uses the most up to date version of Zoom:** In January 2020, Zoom updated its software. In its security update, the teleconference software provider added passwords by default for meetings and disabled the ability to randomly scan for meetings to join.

It should further be noted that no information is stored or transferred via the Zoom platform when executing NYRC's Virtual IME services. Virtual assessments are not recorded and no information (i.e. documents) is shared within the virtual meeting itself. Zoom is used simply as a conduit to facilitate a virtual meeting.

For more information on Zoom's privacy and security credentials please reference the below attachment.

As a leader in delivering IME services throughout Canada NYRC is committed to providing our clients and assessors with Virtual IME services in a safe and secure manner.

If you have further questions about the security and privacy of our services please contact Grace Ma (grace@nyrc.ca) or Matthew Lau (matt@nyrc.ca).

zoom

Zoom and PIPEDA/PHIPA Compliance

At Zoom, we are committed to protecting the security and privacy of our customers' data. This includes enabling our customers in Canada to be compliant with Canadian Data Protection regulations, including the Personal Information Protection and Electronic Documents Act (PIPEDA) and, locally, the Personal Health Information Protection Act (PHIPA).

How does Zoom protect its customers data?

Zoom's commitment to protecting the security and privacy of our customers' data includes:

- Submitting our privacy practices to independent assessment and certification with TrustArc
- Undergoing an annual SSAE-16 SOC 2 audit by a qualified independent third-party
- Performing regular vulnerability scans and penetration tests to evaluate our security posture and identify new threats

What is PIPEDA and PHIPA?

PIPEDA is a Canadian federal privacy law, enacted in April of 2000, for private sector business. It sets rules for how businesses must handle personal data in the course of commercial activity.

Enacted in November 2004, PHIPA is a local, provincial (Ontario) legislation that protects the confidentiality and privacy of personal health information (PHI) by establishing rules for the collection, use, and disclosure of PHI during the provision of healthcare.

What is "personal information" and "personal health information"?

Under PIPEDA, personal information is defined as any factual or subjective information, recorded or not, about an identifiable individual. This includes information, such as:

- Age, name, ID numbers, income, ethnic origin, or blood type
- Opinions, evaluations, comments, social status, or disciplinary actions
- Employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, or intentions (for example, to acquire goods or services, or change jobs)

Under PHIPA "personal health information" means any information related to:

- The provisioning of healthcare services and treatment
- Payment for the provisioning of healthcare services
- Mental or physical health information

Are there any PIPEDA or PHIPA certification programs?

No. Currently there are no PIPEDA or PHIPA certification programs to assess third-party compliance.

Does PIPEDA or PHIPA impose any data localization requirements?

No. Data does not need to remain in Canada in order to comply with either of these privacy laws. As long as adequate transfer mechanisms are in place, Canadian data can be stored in the United States.

How does PIPEDA and PHIPA compare to US (HIPAA) and EU (GDPR) privacy regulations?

PIPEDA is a general data privacy regulation not specifically focused on personal health information, while PHIPA is limited to protecting the privacy and confidentiality of PHI. In that respect, PIPEDA is closer to EU GDPR, and PHIPA aligns to the US HIPAA regulations. However, both Canadian regulations focus on the use, transmission, storage, and security of data in ways that are more similar to the EU GDPR and its requirements for consent, access, transparency, etc. Whereas HIPAA looks to establish Business Associate relationships through BAA contracts that enable third parties to receive PHI in order to perform services, PHIPA requires that third parties ensure adequate protection of the data before they can receive it. And their use of data is limited to the purpose for which it was originally collected. Like GDPR, both Canadian regulations can be complied with by entering Data Protection Agreements which will ensure the adequacy of the data protection mechanisms that support the transfer to data.

How does Zoom help with PIPEDA and PHIPA compliance?

Zoom uses privacy practices and technical security measures to ensure that customer data is protected. Our security and privacy measures include:

- The execution of "Data Protection Agreements" to contractually establish adequate transfer mechanisms
- Providing a variety of in-meeting product security features
- Protecting data in transit by TLS 1.2 using 256-bit Advanced Encryption Standard (AES-256)
- Leveraging the physical and environmental protection of our TIER 1 data center providers. Zoom's hosting facilities have 24x7 manned security and monitoring through multiple layers of physical security controls including perimeters fences, manned lobbies, surveillance cameras (CCTV), man trap, locked cages, motion detectors, and biometric access requirements
- No monitoring, viewing, or tracking of the video or audio content of your video meetings or webinars
- No sharing of customer data with third parties
- Limiting retainment of accounts to 30 days after termination to assist with product reactivation (if requested by customer). After 30 days have passed, the account is permanently deleted

Additional Resources

PIPEDA in Brief
Personal Health Information Protection Act

Security and Privacy Certifications

SOC2:

The SOC 2 report provides third-party assurance that the design of Zoom, and our internal processes and controls, meet the strict audit requirements set forth by the American Institute of Certified Public Accountants (AICPA) standards for security, availability, confidentiality, and privacy. The SOC 2 report is the de facto assurance standard for cloud service providers.

TRUSTe:

TRUSTe has certified the privacy practices and statements for Zoom and also will act as dispute resolution provider for privacy complaints. Zoom is committed to respecting your privacy. If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third-party dispute resolution provider (free of charge) at https://feedback-form.truste.com/watchdog/request.

EU-US Privacy Shield:

Zoom participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework. Zoom has committed to subjecting all personal data received from European Union (EU) member countries, in reliance on the Privacy Shield Framework, to the Framework's applicable principles. To learn more about the Privacy Shield Framework, visit the U.S. Department of Commerce's Privacy Shield List https://www.privacyshield.gov/list.