Appendix A
TECHNICAL SPECIFICATIONS AND DATA POLICY

Technical specifications:

This Appendix A describes the technical requirements to use Dialogue's software platform and medical record systems to provide medical services to Dialogue members.

Physical requirements: Consultations should be done from a private, closed space.

Hardware:
- Computer with the latest version of an operating system approved by Dialogue (Windows or Mac OS). If applicable, an automatic operating system update and hard disk encryption must be properly configured and enabled.
- Built-in or external webcam.
- Built-in or external microphone.

Software: Google Chrome Web Browser with the default configuration and automatic updates enabled.

Malware protection: You will be provided with Malware protection software (SentinelOne Agent) which you must install on your computer. Dialogue will provide installation instructions and assistance with installation if required. System malware protection must be enabled at all times on your device.

Connectivity: Reliable, constant connection with a minimum of 10 Mbps or higher speed for upload and download is required.

Data Policy:

Data Storage: You commit to never store any personal health information (PHI) or data on any of your devices. With the exception of Custodians practicing in Alberta, you hereby acknowledge and agree that such PHI and data remain under the control of Dialogue's managed Care Platform application (which never persists this data to disk).

Data Transmission: Transmission of member PHI shall only be through Dialogue's Care Platform or its approved medical record systems.

Connection to the Care Platform: Connection shall be done only through secure WiFi (802.11 WPA2 with strong, non-default passphrase or Enterprise configuration) that is under the control of the health service provider or a trustworthy service provider (i.e. not a public WiFi access point).

Data Storage: You agree to never store any PHI on any device unless the device is fully encrypted to accepted standards and secured by a strong password.

Endpoint protection: All communications and storage devices must be protected with a strong device password (as defined in section 13.1 of the Information Security Policy) and must never be left unattended or unlocked in an insecure area.

Data Security: Passwords must meet minimum standards set by regulation and/or legislation and be kept secured.

I hereby confirm that I accept the terms and conditions stated above, and I have signed the agreement on this

day ___________________.

____
NAME