Department of Evaluation and Research Services
Suite 400, Central City Tower
13450 – 102nd Avenue
Surrey, B.C. V3T 0H1
Tel: 604.587.4413 | Fax: 604.930.5425

Fraser Health Guidance for Researchers using Virtual Tools and Teleconferencing Options[1]

Fraser Health researchers have access to a wide variety of platforms that staff can access and use for research purposes in order to comply with current public health directives to avoid face-to-face or in-person meetings. In addition, those researchers with affiliations at other institutions may have additional guidance and tools they can use or access. In these instances, please refer to those institutions for other guidelines or recommendations.

Fraser Health staff are expected to use Fraser Health compliant versions of these platforms rather than the public versions in order to meet ethical principles including confidentiality. Privacy is also a consideration and adherence to Health Authority based requirements must be met.

General Ethical Advice on using Virtual tools, Video and Audio Conferencing

- Video images are considered identifiable information. Special care should be taken when video is to be used in research.
- The protocol and consent documents should state who will have access to images and recordings, if they are taken.
- Articulate in the application, protocol, and consent documents what the methods will be to protect the participant's identity including whether images or voices will be distorted.
- When images or voices of individuals may require assent, researchers should provide a detailed explanation and rationale if the researcher plans to depart from this normal practice. The storage and use of unaltered images or recordings must be clearly explained in the consent and assent forms.
- Consider where and how long the images or recordings will be stored and disclose this in the application including relevant study documents.
- Is future use something that may occur? If so, participants should be informed and an option provided to consent or not for future use.
- Where future use may include non-research related purposes then a separate release (e.g. photo release form) should be included with the consent documents.

[1] This guidance has been developed by Island Health's Research Ethics Office and has been adapted for use at Fraser Health with permission. The Fraser Health Research Ethics Office extends our sincerest appreciation for permitting our use of this resource.

Department of Evaluation and Research Services
Suite 400, Central City Tower
13450 – 102nd Avenue
Surrey, B.C. V3T 0H1
Tel: 604.587.4413 | Fax: 604.930.5425

Consent Document Requirements

Consent forms must be very clear regarding the use of video and audio recording. TCPS 2, Article 5.3 states “In disseminating findings, researchers shall not disclose identifiable information without the consent of participants. “ The consent form must state in clear and lay language how the tool will be used and the precise nature and scope of the consent, which is being given by the participant as it applies to the virtual tool.

The consent form should also make the risks of use of the virtual tool you decide to use clear to your potential participants.

With virtual tools you should specifically consider the following for the tool that you chose to use:

- What are the risk around the information being collected, requested, viewed, changed, stored, or, deleted if others have access to the information.
    - This could be due to a shared device (does anyone else have access to the device),
    - Does the tools vendor have access to the data from the tool,
    - There may be instances where disclosure of information may be required by law or under court order, and
    - Electronic communications can have a higher risk of interception by third parties
- The data may be stored or accessed outside of Canada. This needs to be clear to the individual giving consent
- If you participant needs to have an account to use the virtual tool then they will be creating a relationship with that vendor and will be subject to the privacy and terms of use policies of that company which may be subject to change. This should be explained to them in your consent.

As a researcher you are responsible for ensuring that you are adequately informing you participant of the risks associated with the virtual tool you chose to use. The Research Ethics Boards will expect to see this type of information in your application if you are using virtual tools.

Identity Validation

Ensure that you are appropriately verifying the identity of the participant before any sharing of personal information. Confirming the identity of the recipient prior to disclosing information digitally assists in preventing the unauthorized disclosure of personal information.

Department of Evaluation and Research Services
Suite 400, Central City Tower
13450 – 102nd Avenue
Surrey, B.C. V3T 0H1
Tel: 604.587.4413 | Fax: 604.930.5425

Devices

Where available, employer-provided devices and applications should be used. In the event that a non-organizational device is used, reasonable security measures must be employed. You should ensure that you do not use a shared device and that you follow good security practice as listed below.

1. Regularly update the operating system and Apps
2. Use built-in security features
    a. Find my phone (locate your phone and remotely wipe the data
    b. Set App permissions to minimize access to unnecessary information
    c. Set App location permissions to 'while using the app' (vs 'always')
3. Avoid connecting to unsecured Wi-Fi networks
4. Download apps only from trusted sources
5. Understand the risks of jailbreaking / rooting
6. Set automatic locks and use a strong password
7. Consider multilayered mobile security solutions

Recording Virtual Sessions

If recording will be enabled this must be clear in the participant consent form and information on where the recording will be stored and if they will be encrypted or transferred and how, needs to be outlined in the research ethics application. All participants should be verbally reminded that recording will occur at the beginning of any session.

If you need to record a session, you should ensure that the recordings is only temporarily stored on the host's device, or, if supported by the Health Authority, on the virtual tool. The host device should also ensure that the recording is not being back-up to another cloud system such as Google or Apple. BC's Office of the Information and Privacy Commissioner (OIPC) has stated that data should only be store on mobile devices as a last resort and must be encrypted, which means any data on a mobile device should be securely transferred to a more permanent and secure location (such as an appropriate limited access shared drive) as soon as possible. Data on a mobile device should be encrypted to an acceptable industry standard

Department of Evaluation and Research Services
Suite 400, Central City Tower
13450 – 102nd Avenue
Surrey, B.C. V3T 0H1
Tel: 604.587.4413 | Fax: 604.930.5425

Virtual Conferencing in Research Security Measures[2]

Research activities requiring the use of a virtual conferencing platform, such as Skype, Microsoft Teams, Zoom, WhatsApp, and FaceTime should also consider the following and outline all of the platform security measures that a project will use in the research ethics submission:

- Avoid sharing meeting links on social media or public outlets (unwanted participants may join or lurk in a meeting that they have no intentions of participating in).
- Avoid using Personal Meetings ID (PMI) to host public events - Your PMI is a permanent meeting room that anyone can pop into and out of at any time
- Manage Screen Sharing - To prevent random people from taking over sharing, restrict sharing to the host
- Lock the meeting - By locking the meeting after it has started, no new participants can join.
- Disable the video if you do no require the video feature for your project. The hosts can block the video capacity of the participant to prevent unwanted, distracting, or inappropriate gestures on video
- Introduce a Waiting Room - The Waiting Room is a virtual staging area that allows you to invite guests when you are ready for them.
- Introduce a password to gain access to the meeting room. This is especially important when the research is sensitive.

Participants should be told that they can protect their identity and increase the protection of their personal information if they do not use their actual name. They can do this by:

- using only a nickname or a substitute name
- they can turn off their camera (if the research allows for this and they would like to do this)
- they can mute their microphone (if it is not needed)

[2] This section has been developed by the UBC Behavioural Research Ethics Board (BREB) and has been adapted for use at Fraser Health with permission. The Fraser Health Research Ethics Office extends our sincerest appreciation for permitting our use of this resource.

Department of Evaluation and Research Services
Suite 400, Central City Tower
13450 – 102nd Avenue
Surrey, B.C. V3T 0H1
Tel: 604.587.4413 | Fax: 604.930.5425

Best practice tips for your participants

The below are suggested best practices meant to help you protect your information once it is in your control. It is important to note that these are general best practices and will not guarantee your information won't be accessed by a third party.

- Protect your passwords! Someone could pose as you by sending us a request from your device or email account
- Use download Apps from trusted sources (Google Play, iStore). If the info you are wanting to communicate is of a sensitive nature, you may want to seek a more secure method of communication
- Delete emails and texts you no longer require
- Use your device settings to control what information your Apps have permission to access
- Avoid sending personal information while using public Wifi
- Use permission controls on your device to ensure that none of your applications (Apps) have unnecessary access to your text messages and/or emails
- Use virus protection on your computer or device, and regularly scan

Virtual Tools available at Fraser Health

If research data is being collected virtually/remotely using the same tool approved as part of standard of care (SOC), please include this information in your research ethics submission.

Video/Virtual Conferencing and Source Data Verification:
Fraser Health staff may use their secure **Microsoft Teams** account. Microsoft Teams has been approved for business and clinical use in Fraser Health. It is the preferred method for remote source data verification. With Microsoft Teams you can attach case report forms or other documents for verification. Sharing de-identified source documents and over the shoulder screen sharing of Meditech data from Microsoft Teams are acceptable.

Please follow the Fraser Health guidelines when using Microsoft Teams.
https://pulse/work-essentials/computers-technology/Pages/Microsoft-Teams-support.aspx

Please note that some staff members may also have the option of using Fraser Health's **Zoom** Licence and/or **Skype for Business**. The Fraser Health Research Ethics Board will also accept the use of a secured and approved platform provided by a Research Ethics BC affiliated institution (i.e. UBC Zoom).

Data Collection Tools:

Checkbox is a professional survey tool for individuals, teams, and enterprises and is available as a hosted subscription or on-premises (installable) software. Checkbox allows users to create skilfully branded surveys, deliver and track invitations, and analyze results from any standard PC or mobile browser. More information can be found here

Department of Evaluation and Research Services
Suite 400, Central City Tower
13450 – 102nd Avenue
Surrey, B.C. V3T 0H1
Tel: 604.587.4413 | Fax: 604.930.5425

REDCap (Research Electronic Data Capture) is a secure application for building and managing online surveys and databases. REDCap is provided free of charge for patient-oriented research teams through the BC Academic Health Sciences Network. More information can be found on the BC SUPPORT Unit webpage.

Secure Data Transfer Portal:
Cerberus is a secure file transfer is a web based service that allows you to share files securely (uploading, sharing, downloading, deleting, renaming, etc.). The system keeps a file for seven days, and then it will be automatically deleted seven days after it has been uploaded. If a user publicly shares a file that has an expiration date that is after the seven day deletion time limit, it will still be deleted. More information and the Cerberus User Guide can be accessed here