Guidance for Researchers using Virtual Tools and Teleconferencing Options

Island 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.

Island Health staff are expected to use the Island 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 also 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.

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 REBs 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.

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 app
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.

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 Island Health

Tool	**Online resources**	**Island Health Supported /User supported**
Skype for Business	https://intranet.viha.ca/departments/imit/servicedesk/online_help/office/Documents/Lync/skype2016_userguide.pdf#search=skype	Island

WebEx and Webex Cloud	https://intranet.viha.ca/departments/imit/servicedesk/online_help/Documents/tel_documents/webex_userguide.pdf#search=webex	Island
Zoom for Healthcare		User, but Island support in development
KiteWorks (SFTP)	https://intranet.viha.ca/departments/imit/servicedesk/online_help/data/Documents/kiteworks_userguide.pdf#search=kiteworks	Island
FaceTime		Island

Virtual tool specific to Clinical Care

Clinical care tool	Online resources	Island Health Supported /User supported
InTouch (BC Virtual Visit)		Island
Jabber (in hospital only)		Island
Telehealth Home Health Monitoring		Island

If you are an Island Health researcher and you are having trouble getting access to these tools please contact There are virtual tools specific to Clinical Care. Please refer to the Virtual Care Resources on the intranet for more details. Please consult with the leads of this area for information if you would like to use them for research purposes at telehealth@viha.ca.

Specific Notes on Zoom and FaceTime

Zoom

Island Health recommends that if you use Zoom that you use Zoom for Healthcare with a host account through one of the Health authorities. The different types of Zoom have different levels of privacy and security.

If using Zoom for research activities, use the following Zoom best practice tips:

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

Disable file transfer and use other, more secure methods to share documents.

If the meeting will be recorded, this must be in the consent forms. If it will be required, it should be justified in the application and protocol.

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.

Outline in your research ethics application the particular control that you will have in place for the use of Zoom.

Care needs to be taken when using Zoom, as personal information is stored outside of Canada. Therefore, participants need to be made aware in writing, in the consent form, that Zoom servers are located outside of Canada, and Zoom stores users' names and usage data outside of Canada.

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 in Zoom. 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)

Zoom for Healthcare has the cloud logging of user data and recording disabled. If the meeting host activates the local recording option, or for those who are unable to access a business licensed version of Zoom and are using the publicly available version, you must ensure that you are not using cloud recording if you are using the record feature on Zoom, and follow the general recommendation for recording outline above.

Facetime

FaceTime has end-to-end encryption, but even on an Island Health devices, the encryption is completely controlled and managed by Apple.

Key things from the FaceTime privacy policy to be aware of:

Your Apple id or phone number may be shown to the people you contact and people can reach you using your apple id and email addresses or phone number on your account.

- For research this may be something that you need to consider for protection of your own personal information or that of your participants.

Apple may record and store some information related to your use of FaceTime to operate and improve apple's products and services.

Apple may record and store information about FaceTime calls, such as who was invited to a call, and your device's network configurations, and store this information for up to 30 days.

Information stored with Apple is stored outside of Canada. Therefore, participants need to be made aware in the consent form that Apple servers are located outside of Canada, and Apple stores users' names and usage data outside of Canada