# Guideline # 26: Videoconferencing Platforms and Research with Human Participants


## Summary

Privacy and information security for the York community are of paramount importance especially as it speaks to research with human participants conducted in the online environment. With most research involving human participants now conducted using remote options (such as zoom and other videoconferencing platforms) additional privacy and cybersecurity concerns must be considered.

While zoom (and other videoconferencing platforms) are convenient and are "critical enablers" of research at this time, there are risks associated with their use. Consequently, only research that is low to moderate risk[1] should be undertaken using these tools. Participants should be made aware of the potential risks associated with the use of Zoom and what alternatives, if any, will be made available to those participants who do not want to participate via videoconferencing.


## Use of Zoom in Research

While security concerns regarding ZOOM were in the forefront of news accounts at the outset of the pandemic and concomitant switch to remote research options, the reality is that all platforms (including Facetime, WhatsApp, Skype, MS Teams, Jitsi etc.) have security issues. From unauthorized third-party access (such as zoom "bombing") to participants' surreptitious recording of communications, the risks to participants' identities, and confidentiality of data can be significant. This is of particular concern for focus groups conducted via a video-conferencing platform as a participant could record the information being provided by other participants.

In an effort to provide some clarity for the research community, the Office of Research Ethics in consultation with the Office of Information Security, offer the following guidance on the use of Zoom (note that similar guidance may be applicable to other videoconferencing platforms. Please contact ORE at ore@yorku.ca or IT at askit@yorku.ca

[1] In this case "low" and "moderate" risk refers to risk to participants of disclosure

York University has institutional licenses for MS Teams and Zoom and researchers are therefore recommended to use MS Teams or Zoom for research activities which involve remote video communications and does not require PIPEDA / PHIPA compliance.

If the videoconferencing meeting needs to meet PIPEDA / PHIPA compliance, Zoom provides Zoom for HealthCare which is a more secure version of the standard Zoom. This version of Zoom is not site licensed and is available at a cost to the researcher.

UIT currently covers the cost of 1 Zoom license (standard and Zoom for Healthcare) per user (staff, faculty, students). For sponsored accounts, there is a recovery cost of $67 per year per account, charged to the department. Please send an email to askit@yorku.ca to activate the zoom license.

**Key Functionality**

As with many collaboration platforms, Zoom offers HD Video and Audio, easy sharing of content, a digital whiteboard, accessibility functions and the ability to record meetings. Meetings can include up to 300 participants and can last up to 30 hours.

Key advantages of using the zoom platform are the ability for people to join meetings using a telephone rather than needing a computer, the digital whiteboard, the ability to use break out rooms in a meeting, and the ability for people external to York to join meetings easily. Zoom meetings are encrypted from end-to-end using the AES 256bit encryption algorithm and TLS tunneling as they connect to and travel through the Zoom cloud servers located in Data Centers across North America.

Zoom for HealthCare enjoys the same features as the zoom standard version but with focus on privacy and security to meet PIPEDA / PHIPA compliance. There are certain administrative, technical, and physical safeguards put in place to ensure the confidentiality and integrity of the session. For example, Zoom for Healthcare meetings will only connect to and travel through cloud servers located in Canada. For more information please contact Office of Information Security.

**Key Concerns: Use of Zoom and Risk for Research with Human Participants**

No online meeting platform is “fully” secure. The use of the Zoom standard version would be considered appropriate for low and medium risk studies, where the risk to participants

should the contents of interviews be released is considered ‘low’ or ‘moderate’. Research in which the risk to participants should the contents of any interviews be released is considered ‘high’ should use Zoom for Healthcare. Recordings, chats, and shared documents in Zoom for Healthcare should be encrypted and stored on the local computer instead of cloud servers.

Consent forms should include language that makes it clear what platforms are being used, and also that no guarantee of privacy of data can be made, so the risks of participation are clear. Consent forms should also include language that participants agree not to make any unauthorized recordings of the content of a meeting / data collection session, and in the case of focus groups remind participants that researchers cannot guarantee that all participants will refrain from recording the session. The York University Informed Consent Form template has specific language that addresses risks of use of Zoom and must be used when using video conferencing platforms.

The consent form should specify what is being recorded (audio only or both audio and video). Unless seeing the participant(s) via video is essential to the data collection methodology, the participant(s) should be given the option to participate in the meetings by audio only. When making recordings, it is important that they are saved to a local computer rather than to the cloud-based service wherever possible. Where recordings must be saved to a cloud, they should be downloaded to local storage and deleted from the cloud immediately.

Any meeting details should not be publicly posted, and should limit access to authorized participants, perhaps through the use of a meeting password or by requiring authenticated access.

Things to consider when using zoom[2]:

“If you are choosing to use Zoom, please carefully consider the following:

1. The software itself has had several security vulnerabilities, some revealed last year and some more recently. Every piece of software has security vulnerabilities and Zoom has proven to be no different. It is important to keep all software (including Zoom) patched and up to date.

[2] Source: Waterloo University, Zoom Guidance

2. There have been media reports of the company sharing certain data they collect from meeting participants with third parties. Some of these issues have already been fixed, and others are in the process of being fixed. The company has released a statement saying that they have never sold such information.
3. Users of the software may be susceptible to having their meetings interrupted by individuals or groups with malicious intent. Advice on preventing this interruption (dubbed "Zoom-bombing") is below and should be considered and applied to any other online presentation software.
4. Zoom does not make use of end-to-end encryption. That is to say, while communications between various clients and Zoom are encrypted, those communications are potentially visible to Zoom employees. While this is true of many platforms, it underlines the importance of the service's privacy policies and practices. Note however, that Zoom has addressing this concern with End-to-end (E2E) encryption.
   Please see: https://support.zoom.us/hc/en-us/articles/360048660871-End-to-end-E2E-encryption-for-meetings

**Mitigating Risks**

There are a number of steps a researcher can take to mitigate the risks posed by conducting research using videoconferencing platforms. The following are just a few that should be employed.

### 1. Configuring a Zoom meeting[3]

When scheduling a Zoom meeting, the following options are recommended:

**Meeting ID**: Generate Automatically

**Meeting Password**: Require a meeting password

**Video**: Both host and participant video should be set to 'off' initially

[3] Source: McMaster University Zoom Guidance Document

**Audio**: Both (unless data collection requires the use of video, participants should be given the option to join by telephone only). Select a Canadian dial in number to minimize accidental costs to participants.

Select the following '**Meeting Options'**

**Mute participants upon entry** (to protect the privacy of participants)

**Enable waiting room** (to prevent uninvited guests)

**Sessions with York U attendees**: Configure your session to require authentication. This is ideal for meetings with YorkU community only. All attendees will be required to authenticate using the PY credentials. Do not use this setting if you have guest speakers.

## 2. Publicizing a Zoom meeting

When publicizing a Zoom meeting, to prevent unwanted guests and protect against '**Zoom bombings'** meeting hosts should not publicize meeting details more broadly than is necessary. Where it is possible to simply email meeting details to participants, this is the recommended method. Where meeting details must be publicly posted, meeting hosts are advised to post password information separately from other meeting details and are cautioned that Zoom includes (hashed) passwords in the URLs that it generates by default, which should be removed prior to posting.

## 3. Recording a Zoom meeting

Meeting hosts should be aware that with enough technical awareness, any participant in a video conferencing meeting (using any platform) has the ability to record the meeting without the hosts' knowledge. Consenting processes should make this clear to all participants.

From the web interface, hosts should log into their account and then click on '**my account'**, '**settings'**, and click on the '**recording'** tab. The following options should be set:

**Local recording** should be 'on'

**Hosts can give participants the permission to record locally** should be 'off'

**Cloud recording** should be 'off'

**Automatic recording** should be 'off'

**IP Address Access Control** should be 'off'

**Require password to access shared cloud recordings** should be 'on'

**Auto delete cloud recordings after days** should be set to 'on' with **the time range** set to no more than 7 days. This is just to ensure any cached recording files are deleted since you are going to be saving recordings locally.

**Recording disclaimer** should be set to 'on'.

**Ask participants for consent when a recording starts** should be set to 'on'.

**Ask host to confirm before starting a recording** should be set to 'on'.

When recording a meeting, which is initiated from within the meeting client, select '**Record on this Computer'** (recordings should not be stored on the Zoom cloud servers). Meeting hosts should be aware that even though you have selected a local recording, some caching of data may be done at the server to allow for the local recording. **All participants should be aware that they are being recorded and should have given their consent for this**.

## 4. Preventing Zoom-Bombing[4]

Zoom bombing is when an uninvited participant joins a Zoom meeting anonymously for the purposes of disrupting the meeting with language and/or sharing disturbing content. To help minimize the potential for this, researchers are recommended to do the following:

1. Use random meeting ID instead of a personal meeting ID.
2. Use the feature to require a passcode for the meeting.
3. Make use of the waiting room feature.
4. Under Schedule Meeting, Enable **Only Authenticated Users Can Join** and choose **Passport York**.
5. Do not re-use passwords for multiple meeting URLs.
6. Do not post zoom meeting links on publicly available sites.
7. Add registration to classes for attendees to register instead of posting a generic zoom meeting URL.
8. Mute all participants that are already in the meeting as well as new participants joining the meeting. Do not allow participants to unmute themselves.

[4] Source: York University Office of Information Security Zoom Guidance document

9. Disable private chat. This is to prevent anyone from getting unwanted messages during the meeting.
10. Restrict screen sharing.
11. Report a participant during a meeting.

    As a host, you can also control who has access to share content as well as ability to unmute or remove participants. See more info from Zoom here.

    Note that only paid accounts can create invite-only meetings.

**For More Information:**

The Information and Security site provides a more detailed guidance document, "Zoom Privacy and Security Guidance".