

Zoom Mediation Conferencing – How to Safeguard Privacy and Confidentiality

Is confidentiality protected on Zoom during an online mediation? The answer to the question is “yes”, provided the Mediator has properly configured the key Zoom settings and implemented a best practices privacy protocol for mediations on Zoom.

This article presents a checklist, which at a minimum must be considered, to give the parties the peace of mind that their virtual communications are protected.

First and foremost, Zoom has been adopted by many healthcare organizations around the globe who use the platform to consult with other providers and communicate with patients.¹ Therefore, any software solution that shares patient information must incorporate a host of security protections to ensure protected health information is safeguarded.²

Zoom encrypts in-meeting content at the application layer using TLS 1.2 with Advanced Encryption Standard (AES) 256-bit algorithm.³

If properly configured, you will see a green lock icon at the top left corner of your screen confirming an encrypted connection.⁴



For dial-in participants joining by phone, Zoom’s data center encrypts the audio.⁵

To reach a level of privacy on Zoom, like that needed for healthcare uses⁶, the Mediator must:

- Enable Encryption for 3rd Party Endpoints
- Disable Cloud Recording
- Enable Encrypted chat

Also, it is important to know, that once the Zoom Mediation is over, no session information is retained on the Zoom routers or on the participants’ devices.⁷

¹ HIPAA Journal, Feb 19, 2018, <https://www.hipaajournal.com/zoom-hipaa-compliant/>

² Ibid.

³ Physician Learning Program “Zoom User Manual” Health Sciences Centre, Calgary, Alberta

⁴ Ibid.

⁵ Encryption for Meetings Overview. <https://support.zoom.us/hc/en-us/articles/201362723-Encryption-for-Meetings>

⁶ Compliancy Group, HIPAA Done Right Is Zoom HIPAA Compliant? <https://compliancy-group.com/> March 17, 2020

⁷ Barolo, P. Why the World’s Top Security Companies Choose Zoom, February 15, 2017 <https://blog.zoom.us/wordpress/2017/02/15/how-zoom-secures-your-meetings/>

ZOOM PRIVACY CHECKLIST FOR MEDIATORS

There are over fifty Zoom settings and protocols that can provide, a safe and secure environment, for mediations.

At a minimum, the ones we consider crucial that also include best practices, are as follows:

1. **Encryption** – Enable end-to-end encryption and make sure all participants log on by a *secure internet connection*. In other words, Starbucks is never an acceptable location. The signed Mediation Agreement should require this as a condition.
2. **Instant Messaging Protection** - Enable end-to-end chat protection so any typed messages exchanged between the lawyer and client, or with other parties, is encrypted. One should also disable auto-saving of chats.
3. **Disable all recording options, cloud storage settings and third-party archiving** – Block everyone from storing session content. If your Zoom window control menu has a “Record” icon at the bottom, then this has not been properly configured.
4. **Require a password and door lock** - When scheduling new meetings and for participants joining by phone, the mediator must enable the password settings. After all participants have logged-in, the Mediator can “lock” the session door to further entry.
5. **Mask phone number** – The Mediator should enable the setting that masks the phone numbers of users dialing into the Mediation. For example: 888****666. Clients likely do not want the other parties to see their mobile or home phone numbers.
6. **Virtual background enabling**.- Since lawyers and clients may be mediating from home, enhanced privacy and professionalism can be achieved by enabling “virtual” backgrounds. Participants can upload any image, like that of their office boardroom, to be their virtual backdrop.
7. **Court Style of Cause in invitations** – Mediators should always insert some reference to the court case heading, so email recipients know that the email invitation originated from the Mediator. This helps avoid clicking on Zoom invitation links from unauthorized senders, known as phishing.
8. **Privacy in the Mediation Agreement** – The standard Mediation Agreement, *inter alia*, should provide that: (1) the video and audio will not be overheard by non-parties, like spouses, unless consent is obtained (2) the definition of protected mediation communications includes video, pictures, file and screen shares and instant chats etc. (3) there is a strict prohibition against saving or recording the Mediation session on any device.

9. **Set up a Waiting Room** – Disable the ability of participants to enter the Mediation space before Mediator arrives to start the Mediation. The Mediator is able to set up a Waiting Room that provides a “cone of silence” for each participant until they are brought into the Mediation by the Mediator.
10. **Set up Private Breakout Rooms** – The Mediator must set up multiple private breakout rooms. In the Breakout Room, the lawyer and client have a protected space for confidential discussions, even when they are participating from different remote locations. The Mediator should set up a specific protocol so parties know when the Mediator is going to enter your private Breakout Room. Also, no other participant can enter your room unless the Mediator allows this to happen. Therefore, your permission should be obtained in advance before others are allowed into your Breakout Room.
11. **Main Room and Chat**- The Mediator should caution participants that video and audio in the Main Room are not secure and open to all participants in the Main Room session space. Enabling encrypted chat is necessary to permit private instant messaging with another participant in the Main Room or another room.
12. **Employ secure digital signature software with Zoom** – When Minutes of Settlement are to be signed, it’s a best practice to use well-known signature software to ease signing and authentication of the execution process. We use DocuSign.
13. **Participant Controls** - For security and safety, the Mediator should understand how to expel someone from the Mediation, mute a mic or stop a video feed and how to put someone back into the Waiting Room.

For further help or questions, please email Jeff Morris at jeff@jeffmorrismediation.com