



Alerts

Practical Tips to Mitigate Legal Risk When Videoconferencing

December 11, 2020

Lawyers for the Profession®

My first grader started distancing learning this fall. The determined teacher spent the first two days training the students on how to mute and operate their cameras. Those first graders are now experts at videoconferencing. Yet many seasoned lawyers still do not understand how to mute.

Always assume you have a hot microphone, even though you appear muted on the screen. If you have a connected monitor and you close the laptop, your microphone may still be on. To mitigate risk, do not have a separate phone conversation while you think you are on mute for a video conference. If you must take a call during a video conference, use a belts and suspenders approach – mute and then go to a different room to take the call.

Be sure to consult your professional conduct rules and ethics guidelines as you navigate through the waters of using video conferencing in your law practice. For starters, competence, confidentiality and supervision are three primary rules that you should consider.

Competence

ABA Model Rules of Professional Conduct Rule 1.1 states, in part: “Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.” Comment [8] further notes that “a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology.”

Attorneys working from home or another remote location are under the same obligations to maintain client confidentiality as they would be in the office.

Confidentiality

A key component of Rule 1.6 (confidentiality of information) is that a lawyer must take reasonable efforts to prevent inadvertent or unauthorized disclosure of client information. This means that a lawyer must maintain a videoconferencing environment so that family members and roommates do not overhear privileged or confidential communications. Sometimes we forget that the walls have ears and that our children know more than we give them credit for. Your teenager is a risk of unauthorized disclosure; do not let them overhear your conversations.

Service Areas

[Counselors for the Profession](#)

[Cyber Security for Law Firms](#)

[Lawyers for the Profession®](#)

[Professional Liability](#)



A lawyer is responsible to ensure that client meetings are confidential. Do not assume that your client is alone. You should watch to see if your client's behavior indicates another person has joined the room. Also consider whether you or your client have distance learners within the vicinity. Even your kindergartener is a potential risk point because the parent of your child's classmate may overhear your discussions through their video conferencing meeting.

Many law parents use smart home listening devices to remind their distance learners to transition to the next class. Do not do this if you discuss confidential or privileged information anywhere near the device. Big brother is listening and by using such devices you risk waiving privilege.

Supervision

Rules 5.1 and 5.3 address the duties of supervising lawyers. This is where training is key. It is never enough that attorneys follow the ethical rules themselves. Now, more than ever, while we are working remotely, lawyers must ensure that staff members using video conferencing are following ethical rules too. Staff members likely do not watch continuing legal education programs or read articles like this. Make sure they understand the risks and comply with instructions.

Additional Practical Tips

With the above foundation in mind, here are some practical tips for mitigating risk while video conferencing:

- Do a 360 degree view of your space to ensure that no confidential or privileged information is in view of the camera.
- Pay particular attention to wipe boards, notes and calendars on your walls – prime sources for inadvertent disclosures.
- Review all available settings to see what you can change to mitigate risk.
- Do not enable the “Hide non-video participants” feature, because then you may not notice when a new person has joined the meeting.
- Enable “Silence system notifications when sharing desktop” to mitigate the risk that attendees will see your notifications.
- Practice using any share screen feature to be sure that you are sharing only what you intend to share.
- Close all programs that are not essential for the meeting and hide bookmarks and other tabs if sharing your web browser.
- Do not use smart devices such as those offered by Amazon Alexa and Google voice assistants in locations where client-related conversations may occur.
- Review and understand privacy policies and terms for the video conferencing platform.
- Follow up with an email or written communication to your client for any critical advice or instructions that you provide during a video conference.
- Be sure that your actual name appears below your video, and not a nickname like Foxy 7.

Prepare your clients to assess these issues before they appear for virtual depositions and mediations. Do a test run with your client before you present them for deposition. Counsel clients not to use their phone because exhibits shared on phone screens are too small to be seen. Confirm that your client's plan works appropriately, that they understand the technology and ensure that they do not share screens.

My sibling taught me an important lesson learned in the Marine Corps: Proper Planning Prevents Poor Performance. Which leads to the key takeaways: Understand the technology, plan ahead, practice and be mindful of your video and audio surroundings.

Reprinted with permission from the October 27, 2020 issue of The Daily Business Review. © 2020 ALM Media Properties, LLC.