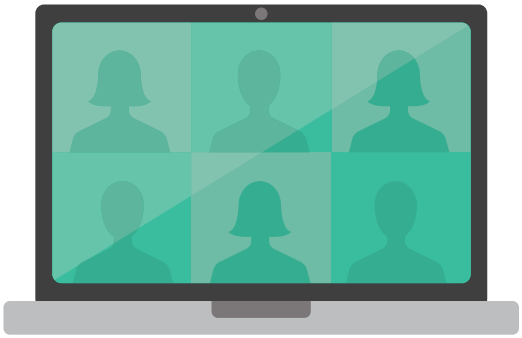
#ForensicPerspectives

E-Discovery Obligations for Videoconferencing



Preservation applies to videoconferencing

Individuals or organizations may be obligated to preserve videoconference recordings, polls, and chat messages if they know or reasonably should know that they will serve as critical evidence in a pending or prospective action. Failure to do so could result in sanctions under Federal Rule of Civil Procedure (FRCP 11, 26(g), and 37).

Know where your video recordings reside

Certain videoconferencing tools often utilize arbitrary file names and folders to save recordings and chats. FRCP 26(b) and 34(a) requires attorneys and clients to identify, collect, and produce electronically stored information (ESI), including teleconferencing and videoconferencing records under, so they should know how and where their files are maintained.

Apply an expansive definition of ESI

ESI is typically considered any data that is stored in an electronic medium and is retrievable in perceivable form. It includes, but is not limited to, email, instant messaging, videoconferencing, and other electronic correspondence (FTC v. Kutzner).

Lawyers must understand the tools and the risks

As part of the obligation to provide competent representation to a client, which requires the legal knowledge, skill, thoroughness, and preparation reasonably necessary for that representation under ABA Model Rule of Professional Conduct 1.1, a lawyer must understand the benefits and risks of using videoconferencing technology to communicate with and provide legal advice.

Know the trajectory of the development of the tool

According to Comment 8 to ABA Model Rule 1.1, "To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology…" As tools update their security, features, and archiving capabilities, lawyers must be aware of these changes and their impact on discovery.

CRA Charles River Associates

Limit the liability of loose protections

ABA Model Rule 1.6(c) requires a lawyer to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." This could include accidentally conducting a video call with private material in the background or accidentally displaying protected documents.

Safeguard the sanctity of the videoconference

Comment 18A to ABA Model Rule 1.6(c) specifically requires a lawyer to "act competently to safeguard information relating to the representation of a client against the unauthorized access by third parties." Be familiar with the array of available tools videoconferencing tools available, select the most secure option, and track their updates and feature changes.

Avoid wrongfully recording attendees

Hosts should be fully familiar with the recording laws of every state where a participant may be located. Only record with full, affirmative consent of each attendee.

Side conversations may be discoverable

On larger videoconferences, attendees may engage in side conversations through the platform's private chat feature or through email, Slack, and instant messaging, among other options. If the subject of that discussion relates to the call in which they are participating, the correspondence may also be discoverable and subject to the same preservation requirements.

Videoconference backgrounds may have relevant information

Individuals often display text in their background, such as contact information, corporate logos, mission statements, and service offerings. These images may be discoverable; however, legal professionals must understand where they are archived to fulfill their preservation obligations.

Privacy is a potent point of confusion

Know the privacy policy parameters of your videoconferencing provider. If you learn that the provider shares personal information with third parties, let the participants know. Some tools may also allow users to change their settings to limit the disclosure of these details.

CRA provides critical expertise in e-discovery, forensic investigations, information governance, and computer forensics. Our Forensic Services team routinely helps companies and their counsel independently respond to discovery requests. Contact an expert listed below to learn more.

Josh Hass, CFE, CEDS
Vice President, Forensic Services
+1-212-520-7139 | jhass@crai.com

Miri Davidson
Principal, Forensic Services
+1-212-520-7282 | mdavidson@crai.com