Best Practices in Providing Virtual Services

Vicky Law

Rise
WOMEN'S LEGAL CENTRE

DISCLAIMER

Nothing we say in this presentation should be construed as legal advice. This is simply for information purposes only. Please consult with a lawyer if you need legal advice.

Agenda

- Potential Risks to Deliver Legal Services via Video-Conferencing
- Security and Safety Concerns for Zoom
- When should you use Zoom or video-conferencing with clients?
- System and Security Requirements for video-conferencing
- Setting up Zoom Meeting with Clients
- Best Practices

Potential Risks to delivering Legal Services via Video-Conferencing

- Risk of compromising confidentiality of documents and legal advice during transmission via video conferencing or email.
- Exposure of information when cloud sharing is enabled on personal devices.
- Unauthorized monitoring and recording of the video conference.
  - Zoom not end to end encrypted: https://theintercept.com/2020/03/31/zoom-meeting-encryption/

Security and Safety Concerns for Zoom

- The collection, storage and access to personal information on Zoom by Zoom staff;
  - https://zoom.us/privacy
- The selling and trading of personal information collected and stored by Zoom;
- Zoom-bombing: people hijacking videoconference meetings
- Signing up for Zoom accounts through other social media accounts (Google or Facebook)

When should you use Zoom (or other videoconferencing) with Clients?

- The other million-dollar question: is there a better software?
- Commissioning affidavits in accordance with the directions from BCPC, BCSC, and BCCA
- You or the client(s) are experiencing difficulties/barriers when using only the telephone to provide and receive legal services

System Requirements

- Computer, tablet or smartphone that is safe and private
- Safe, secure, and stable internet connection
  - You and the client are not sharing WIFI with anyone else you/they don't trust (i.e. landlord/neighbor, etc)
  - If internet is not stable, client can still use video function and call in to Zoom meeting to limit bandwidth
- Webcam
- Microphone and speakers / headsets
- Private room to provide/receive confidential information

Security Requirements

- Firewalled internet connection
- Up-to-date, quality anti-virus and anti-spam programs installed
- If the computer is networked and/or using WIFI, devices are protected from one another

Setting up Zoom Meeting with Client

- Don’t use client’s name in “Topic”
- Generate Meeting ID automatically and use new Meeting IDs for each meeting
- Enable video on for both hosts and participants
- *Email Link to Meeting or provide Meeting ID over the phone?*

Setting up Zoom Meeting with Client (continued)

- *Password embedded in the link?*
  - or disable and provide password through phone or separate email
- Waiting room enabled
- Under “Security tab,” lock meeting when all participants have joined
- Suggested Zoom settings can be found in PDF

Best Practices when using Zoom

- Clients do not need to sign up for Zoom account
- Clients do not need to download Zoom app except on smartphones
  - Clients can attend Zoom meeting by going to www.zoom.us and click “Join A Meeting” at top right corner and entering in Meeting ID and password
- Never record Zoom meetings with clients or even with colleagues when confidential legal matters are discussed
- Do not share documents through the Zoom platform
- Do not provide legal advice or obtain confidential facts through chat option

Best Practices (continued)

- Before the start of the meeting, remind the client that there are risks to videoconferencing and list specific risks
- Remind the client the client that they have the right to stop the videoconferencing meeting at any time
- Ask for and document the client's verbal informed consent
- Ensure that the area behind you, which will be seen by the connecting party, does not reveal anything that may infringe upon the privacy of others (e.g. photos, bulletin boards, binders etc.)

Other types of videoconferencing software

National Network to End Domestic Violence, Video Conferencing & Digital Communication Platforms: Comparison Chart

https://static1.squarespace.com/static/51dc541ce4b03ebab8c5c88c/t/5e7e62a25ed80a4219adad77/1585341091261/NNEDV_Communication+Tools_Handout.pdf

- We are continuing our researching to find alternative solutions

Legal Practices: Client Identification or Verification

Under the *Law Society Rules,* Rule 3-99, lawyers are exempt from identifying or verifying the client's identity when providing pro bono summary advice that does not involve a financial transaction (generally, the receipt, payment, or transfer of money on behalf of the client)

Duty of Technical Competence

Federation of Law Societies of Canada amended *Model Code of Professional Conduct* to add the following commentary to the competence rule (r. 3.1-2):

Model Code of Professional Conduct

[4A] To maintain the required level of competence, a lawyer should develop an understanding of, and ability to use, technology relevant to the nature and area of the lawyer's practice and responsibilities. A lawyer should understand the benefits and risks associated with relevant technology, recognizing the lawyer's duty to protect confidential information set out in section 3.3.

Model Code of Professional Conduct

[4B] The required level of technological competence will depend on whether the use or understanding of technology is necessary to the nature and area of the lawyer's practice and responsibilities and whether the relevant technology is reasonably available to the lawyer. In determining whether technology is reasonably available, consideration should be given to factors including:

- (a) The lawyer's or law firm's practice areas;
- (b) The geographic locations of the lawyer's or firm's practice; and
- (c) The requirements of clients.

QUESTIONS??

Rise
WOMEN'S LEGAL CENTRE

THANK YOU!

Vicky Law
Lawyer
Rise Women's Legal Centre
604-757-7028
vlaw@womenslegalcentre.ca

Rise
WOMEN'S LEGAL CENTRE