Frequently Asked Questions
Ethical Obligations in Remote Working & Remote Legal Services

Prepared by Toby Rothschild, Of Counsel, OneJustice[1]

June, 2020

How can our organization enable staff to fulfill their ethical obligations when working remotely and providing remote services?

The most important ethical issue to consider is the protection of client confidentiality, however organizations should also consider how the changed work environment relates to other ethical obligations such as competence, conflicts of interest and communication with clients. Management should take proactive steps to enable their staff to meet their ethical responsibilities. A written remote working policy should be issued that specifies protocols for protecting client confidentiality and satisfying other ethical requirements. As far as practical, managers and supervisors should provide staff with secure equipment and offer practical guidance on adherence to protocols.[2]

How can our organization maintain client confidentiality when providing remote consultations?

When communicating with clients by phone or video, staff should first ensure that they are speaking to the client (and not another party). Staff should ensure that clients are in a private space before starting any consultation and take special care if there is a potential abuser in the client's home. Likewise, staff should also ensure that nobody else in their own household can see or hear the conversation (including smart devices such as Amazon Alexa or Google Home). Staff should also ensure that client data gathered in the consultation is secure (see below).[3]

Can our organization use third party communication platforms, such as Zoom?

Organizations and staff should identify sensitive categories of information that require additional levels of security. All third-party services should be evaluated prior to use to understand the level of security provided.[4] Services that use end-to-end encryption are the most secure. Staff should use features that reduce the possibility of data breaches, such as password protection for meetings and placing new participants in the waiting room until approved by the organizer.

How can our organization ensure that clients understand information and advice in remote services?

Communicating via phone or video call may make it more difficult for clients to understand information and advice, especially if clients have diminished capacity. At the outset, staff should ensure that (prospective) clients understand whether or not an attorney-client relationship has

---

[1] With appreciation to Peter James of OneJustice for assistance with this project.

[2] See California Rules of Court (CRPC) Rules 5.1 and 5.3 for rules on supervision.

[3] See CRPC Rule 1.6 and Business and Professions Code section 6068 (e) (1).

[4] The Electronic Frontier Foundation is a useful tool for learning about assessing security risk. https://www.eff.org/deeplinks/2020/03/what-you-should-know-about-online-tools-during-covid-19-crisis

been established. Organizations should have a protocol for recording clients' acceptance of retainers when a signature cannot be obtained (e.g. affirmative confirmation via text/email).

Staff should practice active listening and regularly confirm with clients whether or not they understand the advice provided. Staff should confirm advice in writing, however special care should be taken in domestic violence situations or other circumstances in which the opposing party may see the communication.[5]

What steps should our organization take to keep client data secure?
If staff are working from home, they should only use secure password-protected Wi-Fi to access the internet and avoid using public/free Wi-Fi services. Organizations should provide virtual private networks (VPNs) to enable staff to connect to the network securely. Cloud services such as email should be configured to provide enhanced security, such as multi-factor authentication and encryption options. Staff should be encouraged to use strong passwords and to store passwords securely.

Ideally, organizations should provide staff with a secure laptop dedicated to work purposes. If staff do not have access to a work laptop, they should ensure that they have a separate password-protected user login. Staff should maintain the security of any device used for work purposes, for example by keeping anti-virus and anti-malware software up-to-date and avoiding visiting potentially dangerous websites.

Staff should ensure that client information is kept secure, for example by working in a private space and avoiding downloading client information to their computer. The same principles apply to physical client files which should be kept securely and not accessed by other members of the household. When done working on an electronic file or communication, it should be stored on the organization's central computer system, not on the remote laptop. All client information should be deleted from the laptop.

What other ethical responsibilities should we be aware of?
In addition to confidentiality and communication, staff should also be aware of all of their other ethical responsibilities, such as the duty to act diligently in handling client matters[6], the duty to effectively communicate with clients regarding developments in their representation[7], and properly declining and terminating representation.[8] Remote access should also include access to the conflict database, so new clients, adverse parties and witnesses can be readily checked to avoid conflicts.[9]

[5] See CPRC Rule 1.4 regarding communication with clients.
[6] See CRPC rule 1.3.
[7] See CPRC rule 1.4.
[8] See CPRC rule 1.16.
[9] See CRPC rules 1.7 (current clients), 1.9 (former clients) and 1.18 (prospective clients).