An ACTEC Lawyer's Guide to Working Remotely

Particularly During the Nation's COVID-19 Response

Most of us have worked at home and on vacation more than our families want us to. Working from home during the coronavirus pandemic of Spring 2020 is certainly no vacation. We may be working away from our offices for a long time. **We must use our best *technology hygiene* to protect our clients' data.**

If your firm has a proactive IT department, follow its advice. (This article may help you understand the reasoning behind that advice.) If you're in a smaller organization or a solo, here are some tips from the ACTEC Technology in the Practice Committee. As a reminder, we don't promote specific products, but we do review them. Click the link to our online Software Survey. Those reviews don't constitute endorsements, just candid information from one Fellow to another.

It's Not All About Technology

Protecting your clients' confidences means paying attention to your environment. ABA Model Rule 1.6 applies when we work from home and requires us to make reasonable efforts to protect client confidences. For example, take steps to ensure that your family or others don't see or hear confidential information. With parents and children sequestered at home, you may not be able to work from a separate room. You can still **use headphones or earbuds** for confidential audio and video communications with a client or a client's advisors.

If you are disposing of confidential documents, use a document shredder. Many home shredders have limited capacity and overheat quickly. If you need to shred more documents than your home shredder can handle, secure those documents in a safe place and take them back to your office when you can.

Update Everything

You will probably be connecting to the internet with the router that the telecom company sold you when it first set up internet access. **Update its firmware!** Check that it is up to date at least once a day. That router is a crucial gateway to prevent malware from entering your home network. Your telecom vendor may do the updates for you, but you may have to restart the router for that to happen. Most routers have a label that gives you a numerical address (in the form 19n.16n.1n.1n) that you type into a browser. The label may also give the username and password set at the factory. If you didn't reset those defaults when the company delivered the device, type those in and go through the user-interface to reset the router. Then, reset those defaults so no one else can access your router. See https://www.lifewire.com/how-to-encrypt-your-wireless-network-2487653 for more how-to tips.

Bad actors have always considered home networks a weak link in the security chain. They have largely ignored them, however, because it was more lucrative to hack big companies with their vast amount of consumers' financial and health data. With millions working from home and with a growing number of persons facing financial insecurity, it is reasonable to expect home-hacking to increase.

Have an anti-malware program on your computer. **Update its definitions at least once a day and scan your system.** You should be able to set the software to scan overnight so that it doesn't slow you down.

Educate Your Family about Malware from Links and Attachments

The best anti-malware software doesn't protect against people clicking on a link to a funny meme, which may download ransomware or some other malevolent software. Remind your family members not to click on anything they weren't expecting. That's going to be especially hard when we are all desperate for any contact with our friends. Remind yourself and your family that if they receive something unexpected, they should call the sender to confirm they sent it. Experience tells your author that they will understand and they'll probably appreciate hearing your voice.

Use a Virtual Private Network (VPN)

If you have any doubts about the security of your home network, use a VPN to connect to the internet. If you connect directly to your firm's network, your firm probably has set up a VPN for you. But, if you have any Software as a Service (SaaS) vendors, you will be accessing your data through the internet.

You should also use a VPN if you are connecting through a network that you don't manage. That definitely includes a public wi-fi network. That applies when you are working in a hotel room, which is admittedly not likely to be common right now. It could also include a friend's wi-fi network where you don't have the administrative rights to update the firmware.

Use Strong Passwords and Multi-Factor Authentication

- Use long passwords (at least 11 characters) with a mixture of upper-case letters, lower-case letters, and symbols.
- Use a separate password for each application.
- Use a password manager to keep track of them.

- The password manager will even generate the passwords for you.
- Many programs support multi-factor authentication. For example, you might receive a code texted to your phone that you would then enter on your computer. This protects you unless a thief has stolen both of your devices and obtained your password.

Encryption

Encryption can be an important part of a cybersecurity protocol, whether working from the office or remotely. Jim Lamm, Chair of the Technology in the Practice Committee, will be posting an earlier presentation on that topic to the committee's resources for this difficult time in which we find ourselves.

Conference Calls

Make sure your conference call service is secure. Is the data encrypted in transit, i.e., during the call? If the call is recorded by saving it on the provider's servers, is it encrypted at rest? The Advanced Encryption Standard (AES) 256-bit algorithm is a common level of encryption.

Please also practice *conference call etiquette.*

- Listen for sounds in the background. **Mute your microphone as you join the conference.** Dogs may bark at the doorbell sound when a new participant joins a videoconference. After you unmute your microphone, be careful of noises, such as the clickety clack of tying or the students in your family who are either taking their classes online or chatting with their friends.
- Watch your visual background. If you are working from your kitchen table, the bright background of your window will make you a dark figure against that background. Change your seat so that you get to look out that window at the sunshine. Just make sure that you're not showing the world a stack of dishes on your counter.

Signing Documents

Some of us will be asked to fulfill the sad but important role of updating estate planning documents for a dying client. Each of us will have to decide how to protect ourselves from infection if that client has COVID-19. That medical advice is beyond the scope of this article. But we should be prepared.

- Has your state adopted remote notarization?
- Can witnesses observe the testator or testatrix from an adjacent room or do they have to be in the same room?

- Wipe pens and other surfaces down with a sanitary wipe or solution.
- Are there ways to use gloves or other personal protective equipment to shield you from the paper that the person signs?
- What did lawyers in your state do during the Spanish Influenza period?

Conclusion

We are in this together. Please contact the Technology in the Practice Committee with any suggestions to improve or to add to this advice. We'll get it updated.