Tips for Estate Planning Attorneys Who Are Working Remotely During the Coronavirus Situation

James D. Lamm
Lathrop GPM LLP
March 23, 2020

1. If you are unavailable to handle a client's matter due to the coronavirus situation or any other reason, promptly notify the client. Review the guidance in ABA Formal Opinion 482 (Ethical Obligations Related to Disasters).

2. Arrange for receiving and reviewing items delivered to your office address by U.S. mail and other delivery services so that you do not miss important notices or documents. Arrange for access to paper records from the office as they are needed.

3. Obtain and set up appropriate furniture and technology to work efficiently and effectively from your home office. Consider what resources your staff may need to support you remotely. Ensure that you and your staff have access to tech support as needed.

    a. If you are using an office-provided laptop, consider whether to purchase an external monitor, keyboard, or mouse: https://thewirecutter.com/lists/how-to-create-a-full-time-work-space-at-home/.

    b. If you don't already have a printer or scanner in your home office, consider purchasing an appropriate device: https://thewirecutter.com/reviews/best-laser-printer/; https://thewirecutter.com/reviews/best-all-in-one-printer/; and https://www.pcmag.com/picks/the-best-all-in-one-printers. For small scanning jobs, an app on your smartphone or tablet may be sufficient: https://www.cnet.com/how-to/best-scanning-apps-for-android-and-iphone/. For larger scanning jobs, a dedicated scanner or all-in-one printer with an automatic document feeder is a time-saver. Consider how to handle specialty printing situations (*e.g.*, checks payable from your business account).

    c. Set up a comfortable home office working environment with proper ergonomics: https://www.mayoclinic.org/healthy-lifestyle/adult-health/in-depth/office-ergonomics/art-20046169.

4. Make reasonable efforts for you and your staff to protect confidential information. Review the guidance in ABA Formal Opinion 477R (Securing Communication of Protected Client Information).

    a. Consider appropriate physical security measures for your office (*e.g.*, if fewer people or no people are working there now) and for your remote work environment to protect confidential information.

b. Take steps to ensure that other individuals in your remote work environment do not see or hear confidential information.

   i. Work from a room with a door that closes and use headphones/earbuds when appropriate for confidential audio and video communications.

   ii. If others may see confidential information on the screen of your laptop or other device while you are working, use a privacy screen: https://www.3m.com/3M/en_US/privacy-screen-protectors-us/.

   iii. If you are disposing of paper records containing confidential information, use an appropriate document shredder: https://thewirecutter.com/reviews/best-paper-shredders/.

c. Use a secure connection to the Internet and to your office servers and data.

   i. Consider using a secure cloud-based document management system.

   ii. Use your office-provided remote access software to access your office servers and data.

   iii. If you are not working using office-provided remote access software, ensure that you are using a secure connection to the Internet while working.

      (1) If possible, use an Ethernet cable to connect your desktop or laptop computer to your home router. A wired connection to your home router is faster and more secure than a Wi-Fi connection to your home router.

      (2) If you are connecting to your home router using Wi-Fi, make sure that it is secure and encrypted using at least the WPA2 protocol and an appropriate password. The older WEP and WPA protocols are not secure. Now is a good time to check your home router's Wi-Fi settings and make appropriate updates: https://www.lifewire.com/how-to-encrypt-your-wireless-network-2487653. If you are not happy with your home router's Wi-Fi speed or reliability, consider upgrading to a newer Wi-Fi setup: https://thewirecutter.com/lists/the-gear-to-get-reliable-wi-fi-in-any-home/.

      (3) If you are using Wi-Fi to work remotely in a location that is not your home, use a Virtual Private Network (VPN) service to encrypt the connection between your device and the VPN provider if possible: https://thewirecutter.com/reviews/best-vpn-service/ and https://www.pcmag.com/picks/the-best-vpn-services. This prevents others who use the same Wi-Fi network from seeing your data. Some locations that offer free public Wi-Fi access will block VPN

services, and those locations may not be secure for working. Instead, consider using your smartphone to turn its cellular data connection into a Wi-Fi hotspot: https://www.pcmag.com/how-to/how-to-turn-your-phone-into-a-wi-fi-hotspot. Alternatively, obtain a dedicated Wi-Fi hotspot device for secure Internet access wherever you have a cellular data connection: https://thewirecutter.com/reviews/best-mobile-wi-fi-hotspot/.

d. When sending confidential information by email, either attach the confidential information using an encrypted attachment (*e.g.*, an encrypted PDF document that requires a password to open) or use an encrypted email service.

e. Take steps to encrypt confidential information stored on your devices. You can encrypt the entire storage device (hard drive, solid state drive, USB flash drive, etc.) or you can encrypt individual data files or groups of data files.

f. Use two-factor authentication for remote access to your office systems and for as many of your online accounts as possible: https://www.pcmag.com/how-to/two-factor-authentication-who-has-it-and-how-to-set-it-up.

5. Train yourself and your staff about phishing attacks and other cybersecurity risks. Hackers are using the coronavirus situation to increase their attacks. Think before you click on any link or attachment that you receive, even if it comes from someone that you know and trust.

a. If you are concerned about a link that you receive, right-click on the link and copy it (without opening it), then paste the link at the Sucuri SiteCheck website to check for known malware, viruses, etc.: https://sitecheck.sucuri.net/.

b. If you are concerned about an attachment that you receive, save the attachment to your device (without opening it), then upload the attachment to the VirusTotal website to inspect it with over 70 antivirus scanners: https://www.virustotal.com/gui/.

6. Follow safe computing practices that are appropriate for your situation:

a. Do not leave mobile devices unattended.

b. Keep your operating system, anti-virus, anti-malware, and other applications up-to-date: https://thewirecutter.com/blog/internet-security-layers/. Check for updates frequently.

c. Back up your data regularly to protect against a ransomware attack, virus, malware, theft, or a hardware failure: https://thewirecutter.com/reviews/how-to-back-up-your-computer/.

d. Use appropriate security software on your devices (firewall, anti-virus, anti-malware, VPN, etc.): https://thewirecutter.com/blog/internet-security-layers/.

e. Use separate, strong passwords for each of your user accounts: https://thewirecutter.com/reviews/best-password-managers/.

7. Stay connected (from a distance) to your coworkers, clients, clients' advisors, and referral sources while you are working remotely.

   a. Use video or telephone calls to replace in-person meetings when possible: https://thewirecutter.com/reviews/best-video-conferencing-service/.

      i. For video calls, be aware of what else is visible around you. Consider using a photographer's backdrop screen to hide clutter or avoid unnecessary distractions.

      ii. For video calls, consider your lighting. Having a light source in front of you, such as a window or a desk lamp, can properly light your face for the camera and avoid shadows.

   b. Schedule regular check-in meetings with individual coworkers or practice teams, or schedule a practice weekly team social hour by videoconference to stay connected.

   c. Consider using a group messaging service to stay connected to your coworkers as an alternative to email.

   d. Maintain an internal list of coworkers' cell phone numbers to facilitate communications.

8. Schedule times that you will be working, and ask family members to respect those times to avoid interruptions and distractions. Schedule times for breaks. Take time to stretch, move, get fresh air, and stay hydrated.

9. Consider options for executing client documents that protect the health of your clients, you, and your coworkers. Consider using a local courier that offers mobile notary services. Check applicable local law to see if an electronic signature and remote notarization are permitted for will or trust documents. Note that some states are considering legislative changes or executive orders to change will or trust execution requirements during the coronavirus situation. Consider using an electronic signature and remote notarization for documents other than wills and trusts also:

   a. DocVerify: https://www.docverify.com/Products/E-Signatures/E-Notaries.

   b. Notarize: https://www.notarize.com/remote-online-notarization.

   c. NotaryCam: https://www.notarycam.com/.

   d. SIGNiX: https://www.signix.com/secure-electronic-notarization.

10. Other resources for lawyers working remotely:

    a. CDC Interim Guidance for Businesses and Employers to Plan and Respond to Coronavirus Disease 2019 (COVID-19): https://www.cdc.gov/coronavirus/2019-ncov/community/guidance-business-response.html.

    b. ILTA Tips for Working Remotely: https://www.iltanet.org/blogs/ilta6/2020/03/19/ilta-tips-for-working-remotely.

    c. ILTA Working From Home—Best Practice and Suggestions: https://www.iltanet.org/blogs/michael-ertel1/2020/03/11/working-from-homebest-practices-and-suggestions.

    d. Prepare your law firm tech for coronavirus impact: https://www.law360.com/articles/1249268/prepare-your-law-firm-tech-for-coronavirus-impact.

    e. LawSites' list of free products and services to support legal professionals during the coronavirus crisis: https://www.lawsitesblog.com/coronavirus-resources.