Three ethical entanglements while practicing law remotely

By Todd C. Scott

As a lawyer in 2020, it is likely that you've spent much more time during the year working from home than you anticipated. Recent practice management surveys also indicate that it is likely you are contemplating working from home long after the Covid-19 pandemic has subsided. There is no question that 2020 has been a transformative year for attorneys. One of the few professional benefits of this difficult year has been that many lawyers have discovered in themselves the ability to successfully practice law from home and manage their law practice remotely.

For most lawyers, the challenges to practicing law from home in 2020 came swiftly, and the race to identify and embrace the software tools to keep in touch with clients and colleagues was on. Since so many of the tools necessary for good communications, connectivity, and portability were readily available, the self-taught crash-course for successfully practicing law from home had commenced and attorneys were receiving passing grades in record numbers.

However, as with any momentous business disruptions, often the speed to transition systems and technology runs like a hare while thoughtful contemplation about safety, security, and ethical pitfalls for the successful operation of the firm follows behind at tortoise pace. Now that you've been working home for a while, it may be a good time to check up on whether you new, at-home office set-up creates any hazards for you.

When examining working from home risk factors, three concerns rise to the top:

- Have adequate processes and systems been established to reserve client confidentiality and data security in the home office?
- Is proper attorneys supervision and employee oversight from remote locations being maintained?
- Are there cracks in the systems preserving firm financial oversight and integrity?

Each of these concerns are steeped in ethical responsibilities every attorney must regard, and are grounded upon the ABA Model Rules of Professional Conduct. Moreover, the hazards identified pose an increase risk for an attorney error that could likely result in a professional liability claim if adequate precautions are not taken.

1. Preserving client confidentiality in the home office

Your home office is the weak link in your data security plan for several reasons. Your computer devices are likely used for personal as well as business purposes. There's a good chance your devices are also being used by family members, or the data they contain is visible to others in the home. Odds are, your primary at-home work device is not upgraded or security tested as often as the device you would ordinarily use in your firm. And your home firewall or Wi-Fi security is not as robust as the security tools being used onsite at the firm.

Most lawyers understand the responsibility of preserving client confidentiality and are generally cautious when it comes to securing client information from unintentional dissemination to the public.

The general duty to preserve client confidentiality is found in subpart (a) of ABA Model Rule 1.6 Confidentiality of Information. Subpart (a) reads as follows:

> **ABA Model Rule 1.6 Confidentiality of Information**
>
> (a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

The general rule regarding confidentiality of client information is simple and straight to the point, but may not be as helpful when it comes to understanding the limits on securing confidential client data in electronic format. However, the drafters of the Rules expanded on this in Comment 17, providing assistance to lawyers that may be wondering, "How cautious should I be when storing computerized client data?" Comment 17 reads as follows:

> **ABA Model Rule 1.6 Confidentiality – Comment 17**
> **Exercise Reasonable Care**
> "When transmitting a communication that includes information relating to the representation of a client, the lawyer must take reasonable precautions to prevent the information from coming into the hands of unintended recipients. This duty, however, does not require that the lawyer use special security measures if the method of communication affords a reasonable expectation of privacy." **[Comment 17]**

The Comment includes a word that most attorneys find to be a relief when determining the limits of security tools and processes necessary to protect client data – and the word is "reasonable." What that translates to is that attorneys must do what's reasonably necessary to prevent theft of the client data. But "reasonable" is a sliding scale depending on many factors, including what the client desires in terms of data protection. Comment 17 continues:

> "Special circumstances, however, may warrant special precautions. Factors to be considered in determining the reasonableness of the lawyer's expectation of confidentiality include the sensitivity of the information and the extent to which the privacy of the communication is protected by law or by a confidentiality agreement. *A client may require the lawyer to implement special security measures not required by this rule or may give informed consent to the use of a means of communication that would otherwise be prohibited by this rule*." **[Comment 17 Cont'd.]** (Emphasis added.)

Given that lawyers have a responsibility to take reasonable precautions to securing confidential client data, it is important to know minimum standards for network security. When securing your home office data, let's start with the basics.

Your law office network is only as good as its weakest link. And if you have introduced a home computer to the office wide network through a cloud-based data connection, it is vital the precaution you would take securing the integrity of the office network are also applied to the at-home computer.

Therefore, whether it is your PC at home or any of the computers on-site at the office, make sure the following security tools and protocols are always kept up-to-date:

- **Use strong passwords.** The most likely way a hacker will enter the system of your computer is through a login connection that was set up with an old or weak password. Strong passwords usually involve a combination of 8 or more numbers, letters, and symbols that haven't been used in the past, and are changed every 60 days. Password tools such as LastPass work well for creating unique strong passwords and remembering them for you on your computer or any mobile device.
- **Keep antivirus/anti-malware software up-to-date**. Viruses and malware invasions continue to remain a significant threat to any computer system. Finding these invaders hiding in emails, web links, and rogue software has gotten trickier as the disguises used to cover them up has gotten more sophisticated. Make sure the guardian software looking for viruses and malware is kept up-to-date in all computers, including Windows-based PC's and Mac computers.
- **Make sure all computer devices and mobile phones are data encrypted.** Encryption is a process that you must initiate, especially in your mobile devices, after you purchase them. What it does is establish an encrypted data barrier in the device so that, even if the data was successfully obtained by a hacker, it information within the data would be unreadable because it had been encrypted. All devices have a process for encryption and if you take the time to do it once, you will sleep comfortably at night knowing that even if the device is stolen, the data within is secure from any hacker. For Windows users, search for BitLocker and follow the instructions. For Mac users simply use FileVault within your device to initiate data encryption.
- **Always allow Windows to update is operating system automatically.** Most of what you need to protect your system such as firewalls, anti-virus, and anti-malware is already located in your Windows operating system. Therefore, it is critical for the safety of your computer to always allow Windows to automatically run updates when it is recommending you to do so. Critical updates will alert the operating system to new viruses and patch security weakness that may have become exposed by hackers or malware.

Keeping your home office visually secure is a new concept most lawyers haven't had to worry about until they started working from home. An attorney who works remotely should make extra efforts to limit the visibility of their client data from unauthorized persons – whether it is on a computer screen, a file folder, a notepad, or an invoice left in a printer. Best practices include having separate, password protected computers and peripheral devices in a workspace exclusively dedicated to your law practice. Your client's matters deserve privacy from any unauthorized individuals, even if they happen to be members of your immediate family.

2. Supervising attorneys and staff while offsite

For attorneys who routinely supervise associates or staff, finding ways to supervise employees remotely can be a challenge. Of course there are many software and electronic solutions that would help a supervisor keep an eye on a subordinate's activities from afar, but is that the best solution?

Most managing attorneys will say that technical tricks for watching what a staff member is doing at all times is not necessary and will actually promote an atmosphere of distrust. Instead, they will supervise by monitoring the progress of assigned tasks to make sure their staff member who may also be working remotely is meeting their goals in a timely manner.

Regularly scheduled meetings with subordinate attorneys and staff using audio-visual communication tools like Zoom or Microsoft Teams will promote a team atmosphere in the law firm, no matter where people are working, and remind lawyers and staff to stay ahead of critical deadlines and make progress on all legal matters. If necessary, supply staff members with web cams so that meetings will involve eye-to-eye contact and the supervising attorney can better gauge the comfort level of the staff member who is reporting on their work progress.

Attorneys who supervise other attorneys have a duty to make sure the subordinate attorney's activities comply with the Rules of Professional Conduct:

Rule 5.1: Responsibilities of a Partner or Supervisory Lawyer

(a) A partner in a law firm, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that all lawyers in the firm conform to the Rules of Professional Conduct.

(b) A lawyer having direct supervisory authority over another lawyer shall make reasonable efforts to ensure that the other lawyer conforms to the Rules of Professional Conduct.

(c) A lawyer shall be responsible for another lawyer's violation of the Rules of Professional Conduct if:

(1) the lawyer orders or, with knowledge of the specific conduct, ratifies the conduct involved; or

(2) the lawyer is a partner or has comparable managerial authority in the law firm in which the other lawyer practices, or has direct supervisory authority over the other lawyer, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

For attorneys who supervise non-lawyer staff, the duty to supervise can be much more complex if attorneys and staff are not working in the same location. However, frequent discussions between lawyer and staff and analyzing the staff member's work product will go a long way to achieving proper attorney-staff supervision.

Activities that often result in negligence claims against supervising attorneys more typically include defective work performed by the staff member that should have been performed by the attorney. Support staff can often be so go at what they do that attorneys will develop a strong sense of trust and allow them to create and file documents that should always be reviewed by an attorney. Staff oversite by attorneys is also addressed in the Rules of Professional Conduct:

Rule 5.3: Responsibilities Regarding Nonlawyer Assistance

(a) a partner, and a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm shall make reasonable efforts to ensure that the firm has in effect measures giving reasonable assurance that the person's conduct is compatible with the

professional obligations of the lawyer;

(b) a lawyer having direct supervisory authority over the nonlawyer shall make reasonable efforts to ensure that the person's conduct is compatible with the professional obligations of the lawyer; and

(c) a lawyer shall be responsible for conduct of such a person that would be a violation of the Rules of Professional Conduct if engaged in by a lawyer if:

(1) the lawyer orders or, with the knowledge of the specific conduct, ratifies the conduct involved; or

(2) the lawyer is a partner or has comparable managerial authority in the law firm in which the person is employed, or has direct supervisory authority over the person, and knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

3. Financial oversight for on-the-go attorneys

The systems for tracking finances are not only among the most vital for your firm's viability, but they are also among the most complicated. They require multiple participants for safe and effective oversight, multiple processes for seamlessly recording invoices, payments, and expenses, all operating on a strict timeline that turns over every 30 days. Having key participants to the process working apart in their homes may add a level of complexity to the process leading to errors that, left undiscovered, could be fatal.

The blue-print for successfully managing the flow of money in a law practice can be found in your jurisdiction's Rule 1.15 Safekeeping Property. This rule can change significantly from state to state, and is often, when including the detailed comments, the longest, most complex rule in the book. It is purposefully complex and detailed because it serves as a strict, step-by-step guideline for properly managing your client's money. The ABA Model Rule 1.15 Safekeeping Property reads as follows:

ABA Model Rule 1.15 Safekeeping Property

(a) A lawyer shall hold property of clients or third persons that is in a lawyer's possession in connection with a representation separate from the lawyer's own property. Funds shall be kept in a separate account maintained in the state where the lawyer's office is situated, or elsewhere with the consent of the client or third person. Other property shall be identified as such and appropriately safeguarded. Complete records of such account funds and other property shall be kept by the lawyer and shall be preserved for a period of [five years] after termination of the representation.

(b) A lawyer may deposit the lawyer's own funds in a client trust account for the sole purpose of paying bank service charges on that account, but only in an amount necessary for that purpose.

(c) A lawyer shall deposit into a client trust account legal fees and expenses that have been paid in advance, to be withdrawn by the lawyer only as fees are earned or expenses incurred.

(d) Upon receiving funds or other property in which a client or third person has an interest, a lawyer shall promptly notify the client or third person… a lawyer shall promptly deliver to the client or third person any funds or other property that the client or third person is entitled to receive and, upon request by the client or third person, shall promptly render a full accounting regarding such property.

(e) When in the course of representation a lawyer is in possession of property in which two or more persons (one of whom may be the lawyer) claim interests, the property shall be kept separate by the lawyer until the dispute is resolved…

Whether you work in your law practice as a sole practitioner or as a part of a larger office team, it is critical that while transitioning key features of your firm processes – such as working remotely – you take the time to assess roles, identify oversight, and examine the processes for potential flaws and weakness.

If understanding accounting principles, reconciling trust accounts, managing expense and check-writing authority, and balancing the check ledger are not things that you are comfortable with, you should strongly consider involving an accountant or other financial management and invoicing service that will assist you in the assessment process. Sole practitioners may likely benefit the most if they employ invoice or accounting services to handle some of the firm's critical financial processes.

For attorneys in a group practice, there are two key concerns involving financial management when working remotely: Expense control and fraud protection.

Good financial management includes protocols for controlling expenses. Specifically, it means identifying who in the firm has spending authority, what are the limits to individual spending authority, and how will expenses be monitored and verified. Manual systems that require multiple check signers and verifying bank statements worked well in the past for controlling expenses, but they may not be sufficient in a world where members of the firm are often working apart in separate offices.

Financial card services such as Divvy help small businesses control expenses without having to produce and sign a check from a business checkbook. With Divvy, every business purchase happens on a Divvy card, and employees categorize their transactions with a few taps using the Divvy app. Attorneys managing the expenses can control how much the spenders can spend and managers get real-time visibility into budgets. Services like Divvy offer expense management in two forms: "smart cards" that are tangible credit cards that can have daily limits and vendor controls, or "virtual cards" that produce a unique 16-digit card number each time you purchase online. With a virtual card you are better protected in the case of a data breach.

Fraud protection is always a concern for every firm, especially when multiple employees are involved in the handling of firm finances. Professional liability data shows that cases involving employee theft increase during periods of economic recession. You can significantly lessen the chances of theft by a firm employee if you remove the temptations from their daily tasks. Essential fraud protection includes defining key roles for each individual involved in managing firm finances, employing real-time oversight tools like the reporting features in Divvy, and occasionally transferring the bookkeeping duties among firm employees.