PENNSYLVANIA BAR ASSOCIATION
COMMITTEE ON LEGAL ETHICS AND PROFESSIONAL RESPONSIBILITY

April 10, 2020

FORMAL OPINION 2020-300

ETHICAL OBLIGATIONS FOR LAWYERS WORKING REMOTELY

I. Introduction and Summary

When Pennsylvania Governor Tom Wolf ordered all "non-essential businesses," including law firms to close their offices during the COVID-19 pandemic, and also ordered all persons residing in the state to stay at home and leave only under limited circumstances, many attorneys and their staff were forced to work from home for the first time. In many cases, attorneys and their staff were not prepared to work remotely from a home office, and numerous questions arose concerning their ethical obligations.

Most questions related to the use of technology, including email, cell phones, text messages, remote access, cloud computing, video chatting and teleconferencing. This Committee is therefore providing this guidance to the Bar about their and their staff's obligations not only during this crisis but also as a means to assure that attorneys prepare for other situations when they need to perform law firm- and client-related activities from home and other remote locations.

Attorneys and staff working remotely must consider the security and confidentiality of their client data, including the need to protect computer systems and physical files, and to ensure that telephone and other conversations and communications remain privileged.

In Formal Opinion 2011-200 (Cloud Computing/Software As A Service While Fulfilling The Duties of Confidentiality and Preservation of Client Property) and Formal Opinion 2010-100 (Ethical Obligations on Maintaining a Virtual Office for the Practice of Law in Pennsylvania), this Committee provided guidance to attorneys about their ethical obligations when using software and other technology to access confidential and sensitive information from outside of their physical offices, including when they operated their firms as virtual law offices. This Opinion affirms the conclusions of Opinions 2011-200 and 2010-100, including:

- An attorney may ethically allow client confidential material to be stored in "the cloud" provided the attorney takes reasonable care to assure that (1) all materials remain confidential, and (2) reasonable safeguards are employed to ensure that the data is protected from breaches, data loss and other risks.

- An attorney may maintain a virtual law office in Pennsylvania, including a virtual law office in which the attorney works from home, and associates work from their homes in various locations, including locations outside of Pennsylvania;

- An attorney practicing in a virtual office at which attorneys and clients do not generally meet face to face must take appropriate safeguards to: (1) confirm the identity of clients and others; and, (2) address those circumstances in which a client may have diminished capacity.

This Opinion also affirms and adopts the conclusions of the American Bar Association Standing Committee on Ethics and Professional Responsibility in Formal Opinion 477R (May 22, 2017) that:

> A lawyer generally may transmit information relating to the representation of a client over the [I]nternet without violating the Model Rules of Professional Conduct where the lawyer has undertaken reasonable efforts to prevent inadvertent or unauthorized access. However, a lawyer may be required to take special security precautions to protect against the inadvertent or unauthorized disclosure of client information when required by an agreement with the client or by law, or when the nature of the information requires a higher degree of security.

The duty of technological competence requires attorneys to not only understand the risks and benefits of technology as it relates to the specifics of their practices, such as electronic discovery. This also requires attorneys to understand the general risks and benefits of technology, including the electronic transmission of confidential and sensitive data, and cybersecurity, and to take reasonable precautions to comply with this duty. In some cases, attorneys may have the requisite knowledge and skill to implement technological safeguards. In others, attorneys should consult with appropriate staff or other entities capable of providing the appropriate guidance.

At a minimum, when working remotely, attorneys and their staff have an obligation under the Rules of Professional Conduct to take reasonable precautions to assure that:

- All communications, including telephone calls, text messages, email, and video conferencing are conducted in a manner that minimizes the risk of inadvertent disclosure of confidential information;
- Information transmitted through the Internet is done in a manner that ensures the confidentiality of client communications and other sensitive data;
- Their remote workspaces are designed to prevent the disclosure of confidential information in both paper and electronic form;

- Proper procedures are used to secure and backup confidential data stored on electronic devices and in the cloud;
- Any remotely working staff are educated about and have the resources to make their work compliant with the Rules of Professional Conduct; and,
- Appropriate forms of data security are used.

In Section II, this Opinion highlights the Rules of Professional Conduct implicated when working at home or other locations outside of a traditional office. Section III highlights best practices and recommends the baseline at which attorneys and staff should operate to ensure confidentiality and meet their ethical obligations. This Opinion does not discuss specific products or make specific technological recommendations, however, because these products and services are updated frequently. Rather, Section III highlights considerations that will apply not only now but also in the future.

II. Discussion

A. Pennsylvania Rules of Professional Conduct

The issues in this Opinion implicate various Rules of Professional Conduct that affect an attorney's responsibilities towards clients, potential clients, other parties, and counsel, primarily focused on the need to assure confidentiality of client and sensitive information. Although no Pennsylvania Rule of Professional Conduct specifically addresses the ethical obligations of attorneys working remotely, the Committee's conclusions are based upon the existing Rules, including:

- Rule 1.1 ("Competence")
- Rule 1.6 ("Confidentiality of Information")
- Rule 5.1 ("Responsibilities of Partners, Managers, and Supervisory Lawyers")
- Rule 5.3 ("Responsibilities Regarding Nonlawyer Assistance")

The Rules define the requirements and limitations on an attorney's conduct that may subject the attorney, and persons or entities supervised by the attorney, to disciplinary sanctions. Comments to the Rules assist attorneys in understanding or arguing the intention of the Rules, but are not enforceable in disciplinary proceedings.

B. Competence

A lawyer's duty to provide competent representation includes the obligation to understand the risks and benefits of technology, which this Committee and numerous other similar committees believe includes the obligation to understand or to take reasonable measures to use appropriate technology to protect the confidentiality of communications in both physical and electronic form.

Rule 1.1 ("Competence") states in relevant part:

> A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

Further, Comment [8] to Rule 1.1 states

> To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject. To provide competent representation, a lawyer should be familiar with policies of the courts in which the lawyer practices, which include the Case Records Public Access Policy of the Unified Judicial System of Pennsylvania.

Consistent with this Rule, attorneys must evaluate, obtain, and utilize the technology necessary to assure that their communications remain confidential.

C. Confidentiality

An attorney working from home or another remote location is under the same obligations to maintain client confidentiality as is the attorney when working within a traditional physical office.

Rule 1.6 ("Confidentiality of Information") states in relevant part:

> (a) A lawyer shall not reveal information relating to representation of a client unless the client gives informed consent, except for disclosures that are impliedly authorized in order to carry out the representation, and except as stated in paragraphs (b) and (c).
>
> …
>
> (d) A lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client.

Comments [25] and [26] to Rule 1.6 state:

> [25] Pursuant to paragraph (d), a lawyer should act in accordance with court policies governing disclosure of sensitive or confidential information, including the Case Records Public Access Policy of the Unified Judicial System of Pennsylvania. Paragraph (d) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision. See Rules 1.1, 5.1, and 5.3. The

> unauthorized access to, or the inadvertent or unauthorized disclosure of, information relating to the representation of a client does not constitute a violation of paragraph (d) if the lawyer has made reasonable efforts to prevent the access or disclosure. Factors to be considered in determining the reasonableness of the lawyer's efforts include, but are not limited to, the sensitivity of the information, the likelihood of disclosure if additional safeguards are not employed, the cost of employing additional safeguards, the difficulty of implementing the safeguards, and the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use). A client may require the lawyer to implement special security measures not required by this Rule or may give informed consent to forgo security measures that would otherwise be required by this Rule. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]-[4].
>
> [26] 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. 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. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

Comment [25] explains that an attorney's duty to understand the risks and benefits of technology includes the obligation to safeguard client information (1) against unauthorized access by third parties (2) against inadvertent or unauthorized disclosure by the lawyer or other persons subject to the lawyer's supervision. Comment [26] explains that an attorney must safeguard electronic communications, such as email, and may need to take additional measures to prevent information from being accessed by unauthorized persons. For example, this duty may require an attorney to use encrypted email, or to require the use of passwords to open attachments, or take other reasonable precautions to assure that the contents and attachments are seen only by authorized persons.

A lawyer's confidentiality obligations under Rule 1.6(d) are, of course, not limited to prudent employment of technology. Lawyers working from home may be required to bring paper files and other client-related documents into their homes or other remote locations. In these circumstances, they should make reasonable efforts to ensure that household residents or visitors who are not associated with the attorney's law practice do not have access to these items. This can be accomplished by maintaining the documents in a location where unauthorized persons are denied access, whether through the direction of a lawyer or otherwise.

D. Supervisory and Subordinate Lawyers

Rule 5.1 ("Responsibilities of Partners, Managers, and Supervisory Lawyers") states:

> (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.

Rule 5.3 ("Responsibilities Regarding Nonlawyer Assistance") states:

> With respect to a nonlawyer employed or retained by or associated with a lawyer:
>
> (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 in either case knows of the conduct at a time when its consequences can be avoided or mitigated but fails to take reasonable remedial action.

Therefore, a lawyer who individually or together with other lawyers possesses comparable managerial authority in a law firm, must make reasonable efforts to ensure that the firm has in effect requirements that any staff, consultants or other entities that have or may have access to confidential client information or data comply with the Rules of Professional Conduct with regard to data access from remote locations and that any discussions regarding client-related matters are done confidentially.

III. Best Practices When Performing Legal Work and Communications Remotely[1]

A. General Considerations

In Formal Opinion 2011-200, this Committee concluded that a lawyer's duty of competency extends "beyond protecting client information and confidentiality; it also includes a lawyer's ability to reliably access and provide information relevant to a client's case when needed. This is essential for attorneys regardless of whether data is stored onsite or offsite with a cloud service provider." When forced to work remotely, attorneys remain obligated to take reasonable precautions so that they are able to access client data and provide information to the client or to others, such as courts or opposing counsel.

While it is beyond the scope of this Opinion to make specific recommendations, the Rules and applicable Comments highlight that the need to maintain confidentiality is crucial to preservation of the attorney-client relationship, and that attorneys working remotely must take appropriate measures to protect confidential electronic communications. While the measures necessary to do so will vary, common considerations include:

[1] These various considerations and safeguards also apply to traditional law offices. The Committee is not suggesting that the failure to comply with the "best practices" described in Section III of this Opinion would necessarily constitute a violation of the Rules of Professional Conduct that would subject an attorney to discipline. Rather, compliance with these or similar recommendations would constitute the type of reasonable conduct envisioned by the Rules.

- Specifying how and where data created remotely will be stored and, if remotely, how the data will be backed up;
- Requiring the encryption or use of other security to assure that information sent by electronic mail are protected from unauthorized disclosure;
- Using firewalls, anti-virus and anti-malware software, and other similar products to prevent the loss or corruption of data;
- Limiting the information that may be handled remotely, as well as specifying which persons may use the information;
- Verifying the identity of individuals who access a firm's data from remote locations;
- Implementing a written work-from-home protocol to specify how to safeguard confidential business and personal information;
- Requiring the use of a Virtual Private Network or similar connection to access a firm's data;
- Requiring the use of two-factor authentication or similar safeguards;
- Supplying or requiring employees to use secure and encrypted laptops;
- Saving data permanently only on the office network, not personal devices, and if saved on personal devices, taking reasonable precautions to protect such information;
- Obtaining a written agreement from every employee that they will comply with the firm's data privacy, security, and confidentiality policies;
- Encrypting electronic records containing confidential data, including backups;
- Prohibiting the use of smart devices such as those offered by Amazon Alexa and Google voice assistants in locations where client-related conversations may occur;
- Requiring employees to have client-related conversations in locations where they cannot be overheard by other persons who are not authorized to hear this information; and,
- Taking other reasonable measures to assure that all confidential data are protected.

B. Confidential Communications Should be Private

1. Introduction

When working at home or from other remote locations, all communications with clients must be and remain confidential. This requirement applies to all forms of communications, including phone calls, email, chats, online conferencing and text messages.

Therefore, when speaking on a phone or having an online or similar conference, attorneys should dedicate a private area where they can communicate privately with clients, and take reasonable precautions to assure that others are not present and cannot listen to the conversation. For example, smart devices such as Amazon's Alexa and Google's voice assistants may listen to conversations and record them. Companies such as Google and Amazon maintain those recordings on servers and hire people to review the recordings. Although the identity of the

speakers is not disclosed to these reviewers, they might hear sufficient details to be able to connect a voice to a specific person.[2]

Similarly, when communicating using electronic mail, text messages, and other methods for transmitting confidential and sensitive data, attorneys must take reasonable precautions, which may include the use of encryption, to assure that unauthorized persons cannot intercept and read these communications.

2. What is Encryption?

Encryption is the method by which information is converted into a secret code that hides the information's true meaning. The science of encrypting and decrypting information is called cryptography. Unencrypted data is also known as plaintext, and encrypted data is called ciphertext. The formulas used to encode and decode messages are called encryption algorithms or ciphers.[3]

When an unauthorized person or entity accesses an encrypted message, phone call, document or computer file, the viewer will see a garbled result that cannot be understood without software to decrypt (remove) the encryption.

3. The Duty to Assure Confidentiality Depends Upon the Information Being Transmitted

This Opinion adopts the analysis of ABA Formal Opinion 477R concerning a lawyer's duty of confidentiality:

> At the intersection of a lawyer's competence obligation to keep "abreast of knowledge of the benefits and risks associated with relevant technology," and confidentiality obligation to make "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client," lawyers must exercise reasonable efforts when using technology in communicating about client matters. What constitutes reasonable efforts is not susceptible to a hard and fast rule, but rather is contingent upon a set of factors. In turn, those factors depend on the multitude of possible types of information being communicated (ranging along a spectrum from highly sensitive information to insignificant), the methods of electronic communications employed, and the types of available security measures for each method.
>
> Therefore, in an environment of increasing cyber threats, the Committee concludes that, adopting the language in the ABA Cybersecurity Handbook, the reasonable efforts standard:

[2] https://www.vox.com/recode/2020/2/21/21032140/alexa-amazon-google-home-siri-apple-microsoft-cortana-recording

[3] https://searchsecurity.techtarget.com/definition/encryption

> . . . rejects requirements for specific security measures (such as firewalls, passwords, and the like) and instead adopts a fact-specific approach to business security obligations that requires a "process" to assess risks, identify and implement appropriate security measures responsive to those risks, verify that they are effectively implemented, and ensure that they are continually updated in response to new developments.

Recognizing the necessity of employing a fact-based analysis, Comment [18] to Model Rule 1.6(c)[4] includes nonexclusive factors to guide lawyers in making a "reasonable efforts" determination. Those factors include:

- the sensitivity of the information,
- the likelihood of disclosure if additional safeguards are not employed,
- the cost of employing additional safeguards,
- the difficulty of implementing the safeguards, and
- the extent to which the safeguards adversely affect the lawyer's ability to represent clients (e.g., by making a device or important piece of software excessively difficult to use).

A fact-based analysis means that particularly strong protective measures, like encryption, are warranted in some circumstances. Model Rule 1.4 may require a lawyer to discuss security safeguards with clients. Under certain circumstances, the lawyer may need to obtain informed consent from the client regarding whether to the use enhanced security measures, the costs involved, and the impact of those costs on the expense of the representation where nonstandard and not easily available or affordable security methods may be required or requested by the client. Reasonable efforts, as it pertains to certain highly sensitive information, might require avoiding the use of electronic methods or any technology to communicate with the client altogether, just as it warranted avoiding the use of the telephone, fax and mail in Formal Opinion 99-413.

In contrast, for matters of normal or low sensitivity, standard security methods with low to reasonable costs to implement, may be sufficient to meet the reasonable-efforts standard to protect client information from inadvertent and unauthorized disclosure.

In addition to the obligations under the Pennsylvania Rules of Professional Conduct, which are based upon the Model Rules, clients may also impose obligations upon attorneys to protect confidential or sensitive information. For example, some commercial clients, such as banks, routinely require that sensitive information be transmitted only with a password protocol or using an encryption method.

C. There Are Many Ways to Enhance Your Online Security

[4] Pennsylvania did not adopt Comment [18] in its entirety.

While this Opinion cannot provide guidance about specific products or services, its goal is to provide attorneys and law firms with guidance about how they can meet their obligation of competence while preserving client confidentiality. The following subsections of this Opinion outline some reasonable precautions that attorneys should consider using to meet their ethical obligations.

1. Avoid Using Public Internet/Free Wi-Fi

Attorneys should avoid using unsecured free Internet/Wi-Fi hotspots when performing client- or firm-related activities that involve access to or the transmission of confidential or sensitive data. Persons, commonly called hackers, can access every piece of unencrypted information you send out to the Internet, including email, credit card information and credentials used to access or login to businesses, including law firm networks. Hackers can also use an unsecured Wi-Fi connection to distribute malware. Once armed with the user's login information, the hacker may access data at any website the user accesses.

2. Use Virtual Private Networks (VPNs) to Enhance Security

A VPN, or Virtual Private Network, allows users to create a secure connection to another network over the Internet, shielding the user's activity from unauthorized persons or entities. VPNs can connect any device, including smartphones, PCs, laptops and tablets to another computer (called a server), encrypting information and shielding your online activity from all other persons or entities, including cybercriminals. Thus, the use of a VPN can help to protect computers and other devices from hackers.

3. Use Two-Factor or Multi-Factor Authentication

Two-Factor or Multi-Factor Authentication is a security method that requires users to prove their identity in more than one way before signing into a program or a website. For example, a user might require a login name and a password, and would then be sent a four- or six-digit code by text message to enter on the website. Entering this additional authentication helps to ensure only authorized persons are accessing the site. Although these forms of enhanced security may seem cumbersome, its use provides an additional layer of security beyond simple password security.

4. Use Strong Passwords to Protect Your Data and Devices

One of the most common ways that hackers break into computers, websites and other devices is by guessing passwords or using software that guesses passwords, which remain a critical method of gaining unauthorized access. Thus, the more complex the password, the less likely that an unauthorized user will access a phone, computer, website or network.

The best method to avoid having a password hacked is by using long and complex passwords. There are various schools of thought about what constitutes a strong or less-hackable password, but as a general rule, the longer and more complex the password, the less likely it will be cracked. In addition, mobile devices should also have a PIN, pass code or password. The devices

should lock/time out after a short period of time and require users to re-enter the PIN code or password.

5. Assure that Video Conferences are Secure

One method of communicating that has become more common is the use of videoconferencing (or video-teleconferencing) technology, which allows users to hold face-to-face meetings from different locations. For many law offices, the use of videoconferences has replaced traditional teleconferences, which did not have the video component.

As the popularity of videoconferencing has increased, so have the number of reported instances in which hackers hijack videoconferences. These incidents were of such concern that on March 30, 2020 the FBI issued a warning about teleconference hijacking during the COVID-19 pandemic[5] and recommended that users take the following steps "to mitigate teleconference hijacking threats:"

- Do not make meetings public;
- Require a meeting password or use other features that control the admittance of guests;
- Do not share a link to a teleconference on an unrestricted publicly available social media post;
- Provide the meeting link directly to specific people;
- Manage screensharing options. For example, many of these services allow the host to change screensharing to "Host Only;"
- Ensure users are using the updated version of remote access/meeting applications.

6. Backup Any Data Stored Remotely

Backups are as important at home as they are at the office, perhaps more so because office systems are almost always backed up in an automated fashion. Thus, attorneys and staff working remotely should either work remotely on the office's system (using services such as Windows Remote Desktop Connection, GoToMyPC or LogMeIn) or have a system in place that assures that there is a backup for all documents and other computer files created by attorneys and staff while working. Often, backup systems can include offsite locations. Alternatively, there are numerous providers that offer secure and easy-to-set-up cloud-based backup services.

7. Security is Essential for Remote Locations and Devices

Attorneys and staff must make reasonable efforts to assure that work product and confidential client information are confidential, regardless of where or how they are created. Microsoft has published its guidelines for a secure home office, which include:

[5] https://www.fbi.gov/contact-us/field-offices/boston/news/press-releases/fbi-warns-of-teleconferencing-and-online-classroom-hijacking-during-covid-19-pandemic. Although the FBI warning related to Zoom, one brand of videoconferencing technology, the recommendations apply to any such service.

- Use a firewall;
- Keep all software up to date;
- Use antivirus software and keep it current;
- Use anti-malware software and keep it current;
- Do not open suspicious attachments or click unusual links in messages, email, tweets, posts, online ads;
- Avoid visiting websites that offer potentially illicit content;
- Do not use USBs, flash drives or other external devices unless you own them, or they are provided by a trusted source. When appropriate, attorneys should take reasonable precautions such as calling or contacting the sending or supplying party directly to assure the data are not infected or otherwise corrupted. [6]

8. Users Should Verify That Websites Have Enhanced Security

Attorneys and staff should be aware of and, whenever possible, only access websites that have enhanced security. The web address in the web browser window for such sites will begin with "HTTPS" rather than "HTTP." A website with the HTTPS web address uses the SSL/TLS protocol to encrypt communications so that hackers cannot steal data. The use of SSL/TLS security also confirms that a website's server (the computer that stores the website) is who it says it is, preventing users from logging into a site that is impersonating the real site.

9. Lawyers Should Be Cognizant of Their Obligation to Act with Civility

In 2000, the Pennsylvania Supreme Court adopted the Code of Civility, which applies to all judges and lawyers in Pennsylvania.[7] The Code is intended to remind lawyers of their obligation to treat the courts and their adversaries with courtesy and respect. During crises, the importance of the Code of Civility, and the need to comply with it, are of paramount importance.

During the COVID-19 pandemic, the Los Angeles County Bar Association Professional Responsibility and Ethics Committee issued a statement, which this Opinion adopts, including:

> In light of the unprecedented risks associated with the novel Coronavirus, we urge all lawyers to liberally exercise every professional courtesy and/or discretional authority vested in them to avoid placing parties, counsel, witnesses, judges or court personnel under undue or avoidable stresses, or health risk. Accordingly, we remind lawyers that the Guidelines for Civility in Litigation … require that lawyers grant reasonable requests for extensions and other accommodations.
>
> Given the current circumstances, attorneys should be prepared to agree to reasonable extensions and continuances as may be necessary or advisable to avoid in-person meetings, hearings or deposition obligations. Consistent with California

[6] https://support.microsoft.com/en-us/help/4092060/windows-keep-your-computer-secure-at-home

[7] Title 204, Ch. 99 adopted Dec. 6, 2000, amended April 21, 2005, effective May 7, 2005.

> Rule of Professional Conduct 1.2(a), lawyers should also consult with their clients to seek authorization to extend such extensions or to stipulate to continuances in instances where the clients' authorization or consent may be required.
>
> While we expect further guidance from the court system will be forthcoming, lawyers must do their best to help mitigate stress and health risk to litigants, counsel and court personnel. Any sharp practices that increase risk or which seek to take advantage of the current health crisis must be avoided in every instance.

This Opinion agrees with the Los Angeles County Bar Association's statement and urges lawyers to comply with Pennsylvania's Code of Civility, and not take unfair advantage of any public health and safety crises.

IV. Conclusion

The COVID-19 pandemic has caused unprecedented disruption for attorneys and law firms, and has renewed the focus on what constitutes competent legal representation during a time when attorneys do not have access to their physical offices. In particular, working from home has become the new normal, forcing law offices to transform themselves into a remote workforce overnight. As a result, attorneys must be particularly cognizant of how they and their staff work remotely, how they access data, and how they prevent computer viruses and other cybersecurity risks.

In addition, lawyers working remotely must consider the security and confidentiality of their procedures and systems. This obligation includes protecting computer systems and physical files, and ensuring that the confidentiality of client telephone and other conversations and communications remain protected.

Although the pandemic created an unprecedented situation, the guidance provided applies equally to attorneys or persons performing client legal work on behalf of attorneys when the work is performed at home or at other locations outside of outside of their physical offices, including when performed at virtual law offices.