February 17, 2020

Ethics: The ethical implications of technology in your law practice: Understanding the Rules of Professional Conduct can prevent potential problems

Vol. 76, No. 1 / January - February 2020

Melinda J. Bentley

Melinda J. Bentley is Legal Ethics Counsel for the Advisory Committee of the Supreme Court of Missouri.

Implementing and using technology devices and systems in your law practice can be both exciting and daunting. How do you select a device such as a phone, laptop, computer, or other hardware? How do

Media Contact

Farrah Fite
Media Relations Director
ffite@mobar.org
573-638-2251

> *you select a piece of software, case management system, document management system, backup system, or accounting system?*

How do you become competent in making those selections and using those technologies? What if there is a loss of a device or data? How do you train your staff? While the Rules of Professional Conduct (Rules) cannot tell you what to buy, fortunately, they do give you clear standards, and further guidance is provided through the Comments to the Rules to assist you with implementing and using technology devices and systems in your practice.[2] Further, by having a keen understanding of the Rules and Comments, you, as a lawyer, can be proactive in both preventing potential problems and being able to respond efficiently and ethically if a difficulty, large or small, occurs.

Key Ethics Rules: Building A Framework of Understanding

Three key ethics obligations are at the forefront of establishing a lawyer's understanding in order to prevent potential technology problems: competence, confidentiality, and responsibilities regarding nonlawyer assistants.

Rule 4-1.1 – Competence

The first key ethics obligation underlying a lawyer's use of technology is found in Rule 4-1.1, which states that "[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 [6] provides that "[t]o 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." *(emphasis added.)*

Rule 4-1.6 – Confidentiality of Information

The second key ethics obligation underlying a lawyer's use of technology is found in Rule 4-1.6(a), which generally prohibits a lawyer from revealing information relating to the representation of a client unless an exception is met. In 2017, the Supreme Court of Missouri adopted an additional requirement for lawyers in Rule 4-1.6(c) that "[a] lawyer shall make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of the client." Such disclosure or access to confidential client information not only applies to physical information, such as paper documents in a client file, but also to electronically stored information. Think of the large amount of confidential client information lawyers have electronically. That electronic confidential client information makes lawyers' duty of technology competence under Rule 4-1.1 that much more critical.

Reasonable Efforts on Unauthorized Access and Inadvertent or Unauthorized Disclosure. What constitutes reasonable efforts by a lawyer to safeguard confidential client information to prevent inadvertent or unauthorized disclosure, or unauthorized access? Comment [15] provides guidance to Rule 4-1.6(c) that lawyers are required to act competently regarding safeguarding this information. First, Comment [15] specifically creates three categories of safeguarding information from: (1) unauthorized access by third parties; (2) inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client; (3) and/or inadvertent or unauthorized disclosure by those who are subject to the lawyer's supervision. When describing these categories, Comment [15] references Rules 4-1.1 (Competence), 4-5.1

(Responsibilities of Partners, Managers, and Supervisory Lawyers), and 4-5.3 (Responsibilities Regarding Nonlawyer Assistants).

Second, Comment [15] provides factors to consider in determining the reasonableness of the lawyer's efforts, including but 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).

Comment [15] notes that there is no violation of Rule 4-1.6(c) "if the lawyer has made reasonable efforts to prevent the access or disclosure."[3]

Additionally, Comment [15] provides guidance that the client may require the lawyer to implement special security measures that are not required by Rule 4-1.6, but it also notes that a client may give informed consent to forgo otherwise required security measures under Rule 4-1.6. "Informed consent," as defined in Rule 4-1.0(e), requires communication of "adequate information and explanation about the material risks of and reasonably available alternatives to the proposed course of conduct." Per Rule 4-1.0(e), guided by Comment [6], informed consent in this context means discussing the material advantages and disadvantages of forgoing security measures, discussing available options and alternatives, and possibly advising the client to seek other counsel on this decision. Factors as to reasonableness will depend on the experience of the client or if the client is independently represented by counsel.[4]

Further, Comment [15] references that it is beyond the

scope of the Rules to determine if state or federal data privacy laws require additional safeguards over client confidential information, or notification in the event of a loss of electronic information or unauthorized access to such information.

Finally, Comment [15] advises lawyers to consult Rule 4-5.3 (Responsibilities Regarding Nonlawyer Assistants) and its Comments [3] and [4] regarding supervision of nonlawyer assistants outside the firm.

Reasonable Precautions in Transmission. Comment [16] to Rule 4-1.6 notes that a "lawyer must take reasonable precautions to prevent … information [relating to the representation of a client] from coming into the hands of unintended recipients." In offering guidance on this responsibility, Comment [16] provides two factors to consider when determining if the lawyer can have a reasonable expectation of confidentiality: first, the "sensitivity of the information," and second, "the extent to which the privacy of the communication is protected by law or by a confidentiality agreement."

Comment [16] provides that no special security measures are required "if the method of communication affords a reasonable expectation of privacy."[5] Just as with the considerations previously discussed in Comment [15], Comment [16] provides guidance that the client may require the lawyer to implement special security measures that are not required by Rule 4-1.6, but it also notes that a client may give informed consent to forgo otherwise required security measures under Rule 4-1.6. Further, a lawyer may be required to take additional steps to comply with other law, but that is an issue beyond the scope of the Rules.

Rule 4-5.3 – Responsibilities Regarding Nonlawyer Assistants

The third key ethics obligation underling a lawyer's use of technology is found in Rule 4-5.3, which applies to a

lawyer's responsibilities for the conduct of nonlawyers who are "retained by or associated with a lawyer." Rule 4-5.3(a) sets the requirements for firm-wide measures to ensure that partners or lawyers with comparable managerial authority make reasonable efforts to make sure the firm has measures in place to give reasonable assurance that the nonlawyer assistant's conduct is compatible with the professional obligations of the lawyer. Similarly, Rule 4-5.3(b) requires a lawyer with direct supervisory responsibility to make reasonable efforts to make sure the nonlawyer assistant's conduct is compatible with the professional obligations of the lawyer. Per Rule 4-5.3(c), lawyers are responsible for the conduct of nonlawyer assistants who they employ, retain, or associate with if the conduct of the nonlawyer assistant would be a violation of the Rules of Professional Conduct if engaged in by the lawyer and if one of two scenarios is present:

> (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.

Comment [2] to Rule 4-5.3 provides guidance on supervising the conduct of nonlawyer assistants employed by a lawyer, including but not limited to administrative assistants, investigators, law student interns, and paralegals. It describes making sure such assistants receive "appropriate instruction and supervision concerning the ethical aspects of their employment," particularly on preserving confidentiality.[6] Ways to ensure appropriate instruction include written policies and

protocols, as well as regular instruction on the Rules of Professional Conduct and relevant substantive areas of law in which the nonlawyer is providing assistance. Further, specific protocols should be implemented within the law firm to ensure appropriate supervision of the work product of the nonlawyer.

Comment [3] to Rule 4-5.3 provides guidance on using nonlawyer assistants outside the firm who assist the lawyer in rendering legal services to a client, including but not limited to retaining investigative or paraprofessional services, hiring a document management company, sending client documents to a third party for printing or scanning, and using a service based on the internet to store client information. Lawyers using these services still must make reasonable efforts to ensure that the services are provided in a manner compatible with the lawyer's professional obligations, and the extent of those efforts will depend on the circumstances.[7]

Applying the Rules to Potential Technology Issues

The Growing Need for Technology Competence

As provided for in Rule 4-1.1 and its Comment [6], lawyers do have an ethical obligation to be competent in technology, including its risks and its benefits, in a lawyer's practice. For example, a lawyer in Oklahoma was publicly censured in 2016 based on a reciprocal discipline from the United States Bankruptcy Court for the Western District of Oklahoma where the lawyer was suspended for failure to file documents in a manner that was compatible with applicable rules.[8] The lawyer failed to report his discipline in the Bankruptcy Court to the Oklahoma Bar Association and also failed to timely notify his clients of his suspension.[9] During the hearing before the trial panel of the Oklahoma Bar Association's Professional Responsibility Tribunal, the lawyer "acknowledged his problems with the bankruptcy court were caused by his lack of expertise in computer skills and his frustration

trying to meet the federal court's expectations with electronic pleading requirements." The trial panel reported that the lawyer's problems were not with his knowledge of substantive bankruptcy law, but instead "technological proficiency."[10] The Supreme Court of Oklahoma, in issuing its public censure of the lawyer, encouraged him to "continue to improve his computer skills, or better, to hire an adept administrative assistant to do his pleadings."[11]

While hiring adept support staff is helpful in some circumstances when properly supervised per Rule 4-5.3, it is not a substitute for a lawyer's own technology competency as required by Rule 4-1.1. What are some ways to gain technology competency skills? The answers will be different for each lawyer depending on the lawyer's practice setting and level of technological savvy. One of the best ways to gain the requisite skill and knowledge about the risks and benefits of relevant technology for a law practice is by taking continuing legal education programs related to technology.[12] While Missouri does not require that lawyers receive specific minimum continuing legal education (MCLE) credits related to technology competence, it does offer MCLE accreditation of a number of technology programs that help lawyers gain and maintain professional competence as it relates to the practice of law, professional responsibility, or law office management.[13]

There are several resources readily available to help lawyers build their technology competence, including articles, publications, blogs, podcasts, and more. When it comes to these resources, lawyers should be sure to check that they are receiving information from reputable sources that are appropriate for their practice settings.[14] Malpractice insurance providers may also have resources or standards for insureds.

Additionally, lawyers should read the terms and conditions of service carefully for each new hardware or software

item they consider incorporating into their practices to ensure the item has appropriate safeguards for maintaining client confidential information.[15] Further, lawyers should consider consulting an information technology (IT) professional for assistance.[16]

Email and Other Electronic Communications

If lawyers are using email to communicate with clients, they must take reasonable precautions to prevent the unintended interception of confidential client information and should only use email upon proper consideration of Rule 4-1.6 and Comments [15]-[16].[17] While email may be appropriate in some circumstances, other circumstances where the lawyer is transmitting highly sensitive information may require special security measures to comply with Rule 4-1.6.[18] Special security measures may include using email encryption software, placing password protection on attachments, or using "a well vetted and secure third-party cloud based file storage system to exchange documents."[19] Remember that Rule 4-1.6(c) requires a lawyer to "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of the client." In looking to the factors discussed in Comment [15] to Rule 4-1.6 as to reasonable efforts to prevent access or disclosure, consider having a conversation with the client at the outset of the representation to determine if email is an appropriate means of communication. Some points to consider are:

- How do the lawyer and the client want to use email to communicate?
- What information will the lawyer and client be exchanging by email?
- What are the terms and conditions of the platforms that host both the lawyer's email and the client's email? Are the platforms ensuring privacy or are they mining emails for personal information?
- How is the client going to be accessing the email?[20]

On a personal or work phone or computer? Who else has access to that device or the email account?

Consider these points, as well as the sensitivity of the information being transmitted, to determine if additional security measures are necessary or if email should even be used.[21] By asking some of these questions, it should help the lawyer determine if he or she is acting reasonably in using email as a form of communication.

Other forms of electronic communication may include online client portals that have communication features or by texting. Similar questions about confidentiality and appropriateness of the medium should be asked for each of these other potential forms of electronic communication.

Also, lawyers should be mindful that if they are using one of these forms of electronic communication with clients, the correspondence needs to be retained for the client files in accordance with Rule 4-1.22 (Retaining Client Files) and Advisory Committee of the Supreme Court of Missouri Formal Opinions 115 (no withholding of property belonging to the client to enforce payment of fees or expenses) and 127 (scanning client files).[22]

Data Backups, Case and Document Management Systems, and Electronic File Retention

When considering how to backup data, a lawyer should consider the nature of the information to be backed up. Most of it will likely be confidential client information, but it may include items such as trust account records, business records, and much more. Whether a lawyer is considering online (i.e., cloud)and/or on-site backups, those backups pertaining to confidential client information are governed by Rule 4-1.6 and guided by Comments [15] and [16].[23]

Guidance is provided to lawyers regarding cloud backups in Missouri Informal Advisory Opinion 2018-09. It

describes how lawyers need to maintain competence in using relevant technology per Rule 4-1.1, safeguard confidential client information per Rule 4-1.6(c), and supervise per Rule 4-5.3.[24] It also cautions lawyers to read the terms and conditions of service carefully to determine ownership and security of client information and the level of access the attorney and provider will have to that client information. It goes on to describe what constitutes reasonable efforts to safeguard confidential client information while using cloud computing, including but not limited to:

- Security measures protecting confidentiality of client information during transmission and storage;
- Prompt notification of attorney in the event of a security breach or provider's receipt of a subpoena for client information;
- Ownership of data solely by attorney or attorney's firm;
- No access rights by the provider to client information, except as required by law;
- Regular data backup by the provider;
- Handling of client information in the event attorney's relationship with the provider is terminated;
- Compliance with applicable law regarding data storage and transmission;
- Reliable access to data by attorney;
- No access to data by third parties, including advertisers, except as required by law; and
- Domestic storage of data or, alternatively, storage in a jurisdiction subject to United States data protection laws or equivalent.[25]

It also provides guidance that lawyers should review the provider policies and practices periodically, as these can change.[26]

For on-site backups, lawyers should consider such things as the physical security of the equipment storing the confidential information, level of encryption, and

redundancy (the same data being stored in multiple ways in case one system fails). Lawyers should consult with an IT professional to assist in properly setting up and maintaining this system.

Many case or document management systems are now provided by vendors as cloud-based services, though some are still provided for on-site network usage. When selecting a case or document management system, lawyers should consider similar factors as just discussed for cloud or on-site back-ups.

When backing up client information, lawyers should be mindful that they are required to securely store client files for six or 10 years after the completion or termination of the representation absent having an agreement with the client based on informed consent confirmed in writing.[27] The six-year client file retention applies to client files where the representation was completed or terminated on or after July 1, 2016, and the 10-year requirement applies where the representation was completed or terminated prior to July 1, 2016.[28] "Client files, except for items of intrinsic value, may be maintained by electronic, photographic, or other media provided that printed copies can be produced. These records shall be readily accessible to the lawyer."[29] Advisory Committee of the Supreme Court of Missouri Formal Opinion 127 permits the destruction of paper files (except for items of intrinsic value) prior to the expiration of the required retention period if the files are maintained electronically for the required period in accordance with the Rules of Professional Conduct.[30]

Keeping Client Confidential Information Secure on Phones, Laptops, Tablets, Etc.

Just as lawyers have an obligation to secure physical files of clients from unauthorized access, the same is true of electronic files lawyers maintain on portable electronic devices such as phones, laptops, tablets, and other

[31]

similar devices. Whether the devices are those of the firm, or lawyers and employees are permitted to bring their own devices and use them for firm business, reasonable measures may include some of the following suggestions:

- Take reasonable steps to ensure confidentiality by, at a minimum, having strong passwords to access these devices.[32]
- Passwords should be changed periodically.[33]
- Consider additional safeguards such as encrypting the data on these devices, using multi-factor authentication to access firm systems.[34]
- Avoid public Wi-Fi and only choose secure Wi-Fi, as well as consider using a virtual private network (VPN).[35]
- For lost or stolen devices, have a way to remotely disable the devices and destroy the data contained

PO Box 119 326 Monroe
Jefferson City, MO 65102-0119
P: (573) 635-4128 | F: (573) 635-2811
mobar@mobar.org