LEGAL ETHICS & MALPRACTICE REPORTER

Vol. 1 **March 31, 2020** **No. 4**

TABLE OF CONTENTS

FEATURED TOPIC
LAWYERING AND LEGAL ETHICS IN A TIME OF PANDEMIC

We do not yet know to what extent the coronavirus (COVID-19), will spread in the United States. We do know that the virus has had major impacts in other countries including China, South Korea, Japan, Italy, and Iran, among others. In countries that have been significantly affected by COVID-19, governments have focused on containment of the virus and slowing down its spread. They have implemented quarantines, closed school, cancelled events, and warned the populace to avoid contact with each other ("social distancing") as much as possible. As the virus has spread to the United States, so have these containment and mitigation policies.

The spread of a pandemic disease in the United States along with the policies designed to limit and mitigate its spread and effects will have significant impact on the legal profession. Lawyers should be prepared to deal with these impacts—especially since the spread of the virus may take place with little advance notice and containment policies may be implemented just as quickly. As authorities have begun to advise the population to avoid personal contact as much as possible, physicians and health insurers are discussing the potential of using telemedicine as a substitute for in-person physician visits. Lawyers, too, should consider whether they can ethically substitute telephone or online communications (e.g., email, Skype, Facetime, etc.) for in-person visits with clients.

From an ethical perspective, one must ask whether online contact with clients is an adequate substitute for in-person contact, especially in terms of the requirements of Rule 1.1 on competency, Rule 1.3 on diligence, and Rule 1.4 on communication. There is currently little authority as to whether a wholly online lawyer-client relationship will satisfy the requirements of these rules. On the one hand, personal contact with a client is generally deemed to be extremely important. Personal contact is arguably the best way for a lawyer to closely observe his client, read his body language, and, in some instances, establish a bond of trust. On the other hand, in an emergency that makes personal meetings dangerous for both client and lawyer, such considerations may be less significant. The nature of the lawyer-client communications will also play into the decision whether in-person consultation is necessary. In some cases, such as consultation with a criminal defendant immediately before trial, it may be impossible to avoid an in person meeting. In other cases, such as drafting a simple contract for a client, an in-person meeting may be unnecessary.

We must also consider whether there are any court proceedings that can be handled by telephone or online rather than in-person. In what situations will a judge permit substitution of remote communications for in-person contact? These are critical questions for lawyers and the judiciary, as we are now entering into a pandemic

situation that may well endanger millions of people including lawyers, judges, and litigants. It is critical that the Bar have guidance from the proper authorities on these points as soon as possible.

The increased use of telephonic and online communications with clients may also raise confidentiality issues under Rule 1.6. Generally, lawyers must take care to inform their clients of the potential for data breaches when using these communication methods. On occasion, ethics authorities have taken the position that, when the information being transmitted is particularly sensitive, more than ordinary care is required. This information may require the use of encryption or even more drastic measures (such as not using online communications at all). Lawyers may also want to explore online communication systems designed for doctors that comply with HIPPA confidentiality rules (such as VSee). For guidance on these issues, lawyers should consult, in particular, ABA Ethics Opinion 477R. Lawyers may also want to consult ABA Formal Opinion 18-483 concerning data breaches. The extent to which exceptions to rules designed for normal business may be modified or even eliminated is yet to be clear.

It is equally important that lawyers, judges, and others in the legal system do what they can to prepare now. This might include training lawyers, judges, and staff in how to use the tools necessary to facilitate remote contact. Physical facilities can also be prepared to protect lawyers, judges, staff, and litigants (such as isolation areas in jails, interview rooms equipped with barriers to the transmission of the virus, etc.).

A rather more unpleasant subject is the possibility that COVID-19 may cause a significant number of deaths in the United States. Many who are infected by the virus may need to have counsel prepare wills, trusts, or other testamentary documents, and they may wish to do so before their condition worsens to the point that they are unable to do so. Lawyers who specialize in wills and trusts may want to prepare themselves for adopting accelerated schedules to deal with a possible spike in their clients' need for rapid assistance. They may want to remind clients now that they should be sure to have adequate testamentary protection or prepare form documents that can be generated quickly as the need arises. Additionally, most lawyers will not want to meet in-person with infected clients, so they should be prepared to have necessary conversations about testamentary instruments either by telephone or online. This will raise the issues discussed above.

The United States has not dealt with a serious pandemic outbreak for decades. Past pandemics have made it clear that, when one hits, daily life will change—possibly quite radically. Lawyers have fiduciary obligations to their clients and should be prepared to deal with clients' needs in case COVID-19 spreads widely in the U.S. The judiciary, too, must recognize that activities that were routine a month ago will not be safe a month from now. The key to dealing with this pandemic ethically is to do what we can to prepare for what is coming in the months ahead.

TECH TIP
CYBERSECURITY AND CONFIDENTIALITY

by Matthew Beal

Cybersecurity is generally defined as the state of being protected against unauthorized use of electronic data or the measures taken to achieve this state. Unauthorized use includes both the unauthorized access to and the inadvertent disclosure of protected information. As such, cybersecurity considerations should be a key aspect of how rule 1.6 of the Kansas Rules of Professional Conduct is followed

Rule 1.6 addresses the confidentiality of a lawyer-client relationship. Section (c) discusses unauthorized disclosure or access dictating 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 a client." KPRC 1.6(c). Considering the normative practice of maintaining electronic data and communications, this rule has significant cybersecurity implications.

Comment [4] stresses the importance of confidentiality, stating that "[a] fundamental principle in the client-lawyer relationship is that the lawyer maintain confidentiality of information relating to the representation." Confidentiality is important so that "the client is thereby encouraged to communicate fully and frankly with the lawyer even as to embarrassing or legally damaging subject matter. " Comment [5] indicates the reach of the rule and states in part, "the confidentiality rule applies not merely to matters communicated in confidence by the client but also to all information relating to the representation, whatever its source. A lawyer may not disclose such information except as authorized or required by the Rules of Professional Conduct or other law." This duty is permanent. Comment [28] requires that the duty of confidentiality continue after the client-lawyer relationship has terminated

Accordingly, the attorney's approach to confidential client electronic data must be permanent security. That is, access to confidential client information must be controlled, the electronic data needs to be inaccessible to unauthorized parties, the approach must be nuanced enough to cover multiple sources of electronic data, and this cybersecurity must endure perpetually.

Inadvertent disclosure can arise in several forms. In addition to activities such as transmitting a protected document or including such material in discovery, there are wider concerns including unauthorized access to electronic data by employees or other parties. Where some firms may experience nefarious actors intercepting electronic data during transmission, others may have personnel specifically targeted by bad actors to obtain access to materials stored electronically. In all situations, the burden is on the attorney to make a reasonable effort to prevent disclosure.

In preventing unauthorized access and disclosure, what constitutes a reasonable effort? This is marginally answered in comment [26]:

> 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 (c) 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.

The ABA Standing Committee on Ethics and Professional Responsibility provides a bit more guidance in ABA Formal Opinion 477R, "Securing Communication of Protected Client Information." In light of list of considerations offered in the commentary to Rule 1.6, the Committee recommended the following steps lawyers should take to guard against disclosures, including:

1. **Understand the nature of the threat.** Consider the sensitivity of the client's information and whether it poses a greater risk of cyber theft. If there is a higher risk, greater protections may be warranted.

2. **Understand how client confidential information is transmitted and where it is stored.** Have a basic understanding of how your firm manages and accesses client data. Be aware of the multiple devices such as smartphones, laptops and tablets that are used to access client data, as each device is an access point and should be evaluated for security compliance.

3. **Understand and use reasonable electronic security measures.** Have an understanding of the security measures that are available to provide reasonable protections for client data. What is reasonable may depend on the facts of each case, and may include security procedures such as using secure Wi-Fi, firewalls and anti-spyware/anti-virus software and encryption.

4. **Determine how electronic communications about clients' matters should be protected.** Discuss with the client the level of security that is appropriate when communicating electronically. If the information is sensitive or warrants extra security, consider safeguards

such as encryption or password protection for attachments. Take into account the client's level of sophistication with electronic communications. If the client is unsophisticated or has limited access to appropriate technology protections, alternative nonelectronic communication may be warranted.

5. **Label client confidential information.** Mark communications as privileged and confidential to put any unintended lawyer recipient on notice that the information is privileged and confidential. Once on notice, under Model Rule 4.4(b) *Respect for Rights of Third Persons,* the inadvertent recipient would be on notice to promptly notify the sender.

6. **Train lawyers and nonlawyer assistants in technology and information security.** Under Model Rules 5.1 and 5.3, take steps to ensure that lawyers and support personnel in the firm understand how to use reasonably secure methods of communication with clients. Also, follow up with law firm personnel to ensure that security procedures are adhered to, and periodically reassess and update security procedures.

7. **Conduct due diligence on vendors providing communication technology**. Take steps to ensure that any outside vendor's conduct comports with the professional obligations of the lawyer.

Because attorney-client confidentiality is a paramount concern to both the client and the overall effectiveness of the profession and its servants, cyber security must be considered in identifying a reasonably competent approach to electronic data management.

ETHICS & MALPRACTICE RESEARCH TIP
THE BEST LAW JOURNALS FOR ETHICS RESEARCH

Some of the best sources for commentary on current issues in legal ethics are those few law reviews dedicated to this area of the law. The leading legal ethics law reviews are:

Cardozo Public Law, Policy and Ethics Journal
Georgetown Journal of Legal Ethics
Journal of the Legal Profession (University of Alabama)
Notre Dame Journal of Law, Ethics & Public Policy
Professional Lawyer (American Bar Association)

Of the five journals listed, four are published by law schools and staffed by law students. The fifth is published by the American Bar Association and professionally edited. All of these law reviews publish articles on current and perennial topics in legal ethics, written both by

academics and practitioners. All are excellent. Lawyers who do not subscribe to these journals may access them online through various platforms like Westlaw, Lexis, and Hein Online. Tables of contents are, generally, available online at the journals' websites.

When should a practicing lawyer consult these legal journals? The answer is simple: whenever a lawyer needs more than an ethics rule itself and current law on the rule, one should consult law review articles. These articles will not only provide commentary by experts, but they also provide leads for research in the citations and notes.

Although the five listed journals should always be consulted when doing legal ethics research, they are not the only law reviews that include articles on the subject. Indeed, virtually every general subject law reviews occasionally publish articles on legal ethics and malpractice, so a thorough search of all American law reviews is advisable when you want to be certain to have the latest expert views on a question.

BLAST FROM THE PAST
JONATHAN DYMOND ON LAW AND MORALITY

On the danger that lawyers and courts get bogged down in legal technicalities and forge the principles of morality:

> The practice of disregarding rectitude in courts of justice will become habitual. They will go onward from insisting upon legal technicalities to an endeavor to pervert the law, then to giving a false coloring to facts, and then onward and still onward until witnesses are abashed and con-founded, until juries are misled by impassioned appeals to their feelings, until deliberate untruths are solemnly averred, until, in a word, all the pitiable and degrading spectacles are exhibited which are now exhibited in law practice.

For more, consult: J. Dymond, *Essays on the Principles of Morality, and on the Private and Political Rights and Obligations of Mankind* (1834).

Published by JOSEPH, HOLLANDER & CRAFT LLC
Edited by MIKE HOEFLICH