On-Demand CLE

Planning for the Inevitable:
Protecting Your Law Firm In a Crisis
On-Demand Webinar
Approved for 1.0 hour of CLE Ethics Credit (KY)

Courtney Risk, Business Development Specialist for Lawyers Mutual of Kentucky ("LMICK"), presents tips and strategies for attorneys to prepare for the unplanned and unavoidable circumstances that can interrupt practice operations, including extended illnesses, hospitalizations, and natural disasters. Attendees will gain practical tips for preparing for these eventualities. This session will also address succession planning issues and the ethical considerations, including relevant Model Rules of Professional Conduct, that apply to these issues and other life changing events.

Presented by:

Courtney Risk, Esq.
Lawyers Mutual of Kentucky
risk@lmick.com

Courtney recently joined the Lawyers Mutual team after beginning her career in litigation. In addition to her role in client relationship management, she is focused providing relevant risk management resources. Courtney's experience includes litigation, both criminal and civil, as well as transactional work. She has also worked in the insurance industry, training attorneys and other officials in various legal issues.

10503 Timberwood Circle, Suite 213
Louisville, KY 40223

502-568-6100
502-568-6103 fax

lmick.com

Planning for the Inevitable
Protecting Your Law Firm In a Crisis
Lawyers Mutual of Kentucky
www.lmick.com

Materials developed by:
- **Jane Broadwater Long**, Vice President-Claims Counsel, Lawyers Mutual of Kentucky, Louisville, KY
- **Heidi Wagner Dorn**, Of Counsel, Dinsmore & Shohl LLP, Columbus, OH
- **Gretchen Koehler Mote**, Director of Loss Prevention, Ohio Bar Liability Insurance Company, Columbus, OH
- **Andrea Hunt**, Cobb Law PLLC, Louisville, KY

Updates in 2022 by:
- **Courtney Risk**, Business Development Specialist, Lawyers Mutual of Kentucky

---

A. Planning To Protect Clients' Interests In The Event Of The Lawyer's Death, Disability, Impairment, Incapacity, Or Extended Absence[1]

Who?

Each attorney should designate a back-up attorney to handle matters in case of an emergency. It is recommended to develop a written agreement to define the scope and duration of the arrangement, including parameters to act on your behalf to close the practice in the event of death, disability, impairment, or incapacity.

In the meantime, if you have not identified who your back-up would be, make this a priority. If you have identified your back-up, reach out and set a time to discuss the agreement and confirm it is still a good fit. When determining the best fit, first identify an attorney you trust. Additionally, identify an attorney that:

- has the appropriate qualifications to handle the matters in your practice;
- has the capacity to take on the caseload outlined in the agreement;
- is licensed to practice in Kentucky (and any other jurisdictions you also practice);
- is in good standing with the KBA (and any other applicable jurisdiction);
- is unlikely to have conflicts with you; and,
- has sufficient professional liability insurance.

What?

How would the back-up attorney determine what files are active if you were unavailable? If you utilize a case management or docketing system that only backs-up

[1] Adapted from LMICK's Disaster Preparedness Series, 2022

to a local server, the information could be compromised or lost in a natural disaster. Consult your IT personnel to determine the best option for a secondary back-up. Options for back-ups can range from uploading to a cloud server to routinely printing a docket of all active cases ***as well as client contact information***.

When considering cloud storage options, review the ethical obligations and considerations for cloud computing, here.

When?

Would the back-up attorney be able to easily identify immediate deadlines, court appearances, or other critical meetings? Maintaining a calendar that backs-up to the cloud is often the best choice for ensuring you or your back-up attorney can meet critical deadlines, even if local servers or case management systems are damaged or destroyed. The calendar can also act as a triage guide when the unexpected has occurred, ensuring the most critical items are addressed first.

Preparing Your Agreement with Your Back-Up Attorney

After you have identified an appropriate back-up attorney and reached a verbal agreement, we recommend formalizing the agreement in writing. Once executed, we also recommend updating client engagement letters to notify them of the arrangement as discussed below.

Checklist: *What to Include in the Written Agreement*

- State the purpose and intent of the agreement. The purpose should be limited to only addressing the duties of the back-up attorney in your absence. Include language clarifying that the agreement is not intended to create a partnership or law firm.

- Define the scope of the agreement. Although most attorneys will have a single back-up attorney, it is possible one attorney may be the right fit to help wrap-up your practice in the event of your death or disability while a second attorney may be better suited to cover you on shorter or planned leaves. You may also desire to have the scope limited to certain matters (litigation only, transactional matters only, etc.). Once you determine the best fit for your practice, describe it in the written agreement.

- Determine fee arrangements. The agreement should cover when and how much the back-up is to be compensated. Many attorneys agree to perform back-up services for no or nominal compensation, which should be memorialized in the agreement. If a fee will be shared, consider the time spent on the matter by you, the back-up, and whether the case is on a contingency fee basis. Identify the source of payment, e.g., accounts receivable, settlements, or fees received for the

back-up's services only. It is almost certain that SCR 3.130(1.5(e)) on fee sharing will apply. Be sure to comply with its disclosure and client consent provisions.

- Discuss how client funds will be handled. Consider making arrangements for the back-up to handle your client trust account. One way is to make the back-up a signatory on the trust account. A better way is a special power of attorney that permits the back-up to act for you only in specified circumstances.

- Outline any administrative or practice management duties. For solo practitioners without administrative staff, will the back-up also be handling payment of your office utilities or other firm bills? Are there other tasks that are not client-facing but still need to be handled? Provide a general description of these items and your expectations of the back-up attorney.

- Identify what information has been exchanged. Document what information you have shared. This could include items such as:
    - Law office entry permission and information
    - Professional calendar location and access
    - Client file information and access
    - Contact information for our professional liability insurance provider including the policy number
    - Contact information for key persons to be notified other than clients (which you may want to simply list in the agreement for ease of access)

Additional considerations

If the reason for closing a practice is the death of a sole practitioner, planning agreements designating a closing lawyer may become void. It will probably be necessary for the estate's executor to authorize the designated lawyer to close the practice. For this reason, part of the planning process should include making sure there is a provision in the lawyer's will directing the executor to appoint the designated lawyer to close the practice.

Client Engagement Letters and Back-Up Attorney Arrangements

Back-up arrangements may be implemented only with client consent. The best practice is to notify clients of the identify of your back-up attorney and the agreed upon scope of his or her work in advance in an engagement letter acknowledged in writing by the client. This has the advantage of in-place client consent for a back-up to take over a matter without delay. Remember to update this clause in your engagement letter if this back-up attorney changes. Additionally, if the back-up attorney changes during the course of representation, provide written notice to those existing clients of the change and request their consent.

Sample Clause for Engagement Letter:

Back-up Attorney Notice: In order to meet my ethical obligation to protect your interests in the event I am unavailable due to an extended leave, I have appointed [INSERT NAME HERE] to act as my back-up attorney. [INSERT NAME] will have the authority to [DESCRIBE SCOPE HERE. *EXAMPLE: handle matters that arise during a planned leave and will step in to assist wrapping up my practice should the need arise.*]

Checklist: *Preparing Information for Your Back-Up Attorney*

Now that you have identified your back-up attorney and executed a written agreement, what information do they need to effectively perform their duties and fill-in for you?

We recommend compiling information on both the administrative and the practice procedures. For solo practitioners, this information can reside in a single document. However, for attorneys that have associates that are not involved in certain administrative tasks, the division can allow the practice procedures to be shared for practice management purposes, not only for disaster preparedness.

1. Have a thorough and up-to-date ***administrative procedures manual*** that includes information on:
    a. Client Information:
        1. How to generate a list of active client files, including client names, addresses, and phone numbers
        2. Where client ledgers are kept
    b. Financial Records:
        1. Where the safe deposit box is located and how to access it
        2. The bank name, address, account signers, and account numbers for all law office bank accounts
        3. The location of all law office bank account records (trust and general)
    c. Management Information:
        1. Contact information for your power of attorney and the executor of your estate
        2. Location of documents related to the ownership of the firm, including leases, a list of utilities, etc.
        3. Where insurance policies are located and names of carriers
        4. Procedures for payroll, if any
        5. List of employee benefit providers, if any (i.e., health insurance, retirement, etc.)
    d. Communications:
        1. Where to find, or who knows about, the computer passwords
        2. How to access email accounts
        3. How to access docket or practice management software, if any
        4. How to access your voice mail (or answering machine) and the access code numbers

5. Where the post office or other mail service box is located and how to access it.

e. File Management
    1. Where are files located
    2. Where are the file back-ups located
    3. Contact information for anyone needed for file access

2. Have a thorough and up-to-date ***practice procedures manual*** that includes information on:
    a. How to use the calendaring system
    b. How to check for a conflict of interest
    c. How to use the docket or practice management system
        1. Note: include any contact information for software support or direction to tutorials available from the vendor
    d. How the open/active files are organized
        1. What are the typical subfolders in matters (i.e., client communications, pleadings, research, notes, etc.)
        2. General guidelines for what is saved digitally versus paper copy, etc.
    e. How the closed files are organized and assigned numbers
    f. Where the closed files are kept and how to access them
    g. Where original client documents are kept
    h. The office policy on keeping original client documents

Making Arrangements for Extended Leave[2]

1. Agreement with a Backup Lawyer (See above).

2. Client Considerations

- Backup arrangements may be implemented only with client consent. The best practice is to notify clients in advance. Many lawyers do this in an engagement letter acknowledged in writing by the client. This has the advantage of in-place client consent for a backup to take over a matter without delay. Some lawyers send a letter to clients shortly prior to extended leave informing them of the absence, explaining backup arrangements, and asking for client consent. In either case the backup lawyer should always notify clients immediately upon taking over.
- Protecting client confidentiality is paramount. In sudden emergencies such as the death of a lawyer it is permissible for an unassociated lawyer to inspect the lawyer's client files without client consent to the extent necessary to identify clients and determine matters that require immediate attention. With a long lead

[2] Adapted from "Risk Management Checklists for Maternity Leave" 2015, Lawyers Mutual of Kentucky. Available at http://www.lmick.com/item/risk-management-checklists-for-maternity-leave-3.

time, there should be ample opportunity to get client consent and avoid any question of breach of confidentiality.

3. Your Risk Management Actions Prior to Extended Leave

- The goal is to be sure all active cases have up-to-date files, are accurately calendared, and in a posture to be continued without interruption. This is best accomplished by completing detailed case management plans for every active matter that includes a description of work done and a schedule for accomplishing remaining work. This also helps to determine how fees could be shared with the backup.
- In a perfect world, every practice has a written law office procedures manual or standing operating procedure – in this world relatively few do. If your practice does not have written procedures, you should prepare them for your backup. See above for details about what to include in the written procedures.
- Additionally, for planned absences (parental leave, planned medical procedures, longer than normal travel, etc.) provide your back-up attorney with a ***case memo*** for each case discussing:
    - Key facts
    - Deadlines
    - Client contact information
    - Drafts of upcoming work product that is due
    - Any additional relevant information

Checklist: Preparing For Extended Leave

- ☐ Notify clients.
- ☐ Notify professional contacts.
- ☐ Notify malpractice carrier.
- ☐ Prepare employee(s).
- ☐ Print a master client/contact list.
- ☐ Prepare case status summaries.
- ☐ Arrange for collection of mail.
- ☐ Arrange for payment of bills.
- ☐ Arrange for processing of payments received.
- ☐ Update voice mail and email messages.
- ☐ Update calendar.
- ☐ Place a sign on your door.
- ☐ Map your files.
- ☐ Backup your data.
- ☐ Plan for emergencies.
- ☐ Prepare for the inevitable.

B. Law Firm Succession

Kentucky Guidance for Sudden Departures from Practice[3]

1. SCR 3.395, Appointment of Special Commissioner to Protect Clients' Interests

Key Provisions:

- When it comes to the attention of the [KBA] Director that: ... (c) an attorney has resigned ... and has failed to notify his... clients of his... resignation as required by Court order; or (d) an attorney dies; or (e) an attorney abandons his... law practice or his... whereabouts are unknown, and no law partner, personal representative of the deceased attorney's estate, or other responsible person capable of conducting the attorney's business affairs is known to exist, the Director may petition the [Supreme] Court, and the Court for good cause may order the appointment of one or more members of the Association to serve as Special Commissioners of the Court.

- A Special Commissioner appointed under this rule may be authorized by the Court to take possession of the files and records of an attorney described in subsection (1) above, to make an inventory of the files, to give notice to the attorney's clients of the unavailability or inability of the attorney to continue to represent the clients, to deliver to the clients all papers and other property to which the clients are entitled, to take any other action which the clients are entitled and to take any other action which the Court deems necessary to protect the interests of the clients.

The clear policy of the rule is that appointing special commissioners is a last resort – to be done only when all other options to close the practice are exhausted. The rule's procedures are time consuming, and given the inevitable time lag before notice to the KBA, an appreciable period of time will elapse before a special commissioner can be appointed. The risk for clients during this period is obvious. Adding to the complexity of the situation is that Kentucky does not have a written guide for special commissioners or others to facilitate closing a practice. Under these circumstances, the need for a client protection plan for sudden departures could not be clearer. Bar procedures are simply not designed to cover more than the most desperate situations.

2. KBA Ethics Opinion 405 (1998).

KBA Ethics Opinion 405 is of some help for sudden lawyer departures. It concerns the unusual situation of the death of a sole practitioner whose practice included employed lawyers with no proprietary interest in the practice. These lawyers sought advice on

[3] Excerpted from "What Happens to your Clients if Something Happens to You? The Ethics and Risk Management of Leaving the Practice of Law." Lawyers Mutual of Kentucky, 2004. Available at: http://www.lmick.com/item/what-happens-to-your-clients-if-something-happens-to-you-checklists-for-closing-a-practice.

their professional duty to firm clients. Of primary interest for this article is the adoption in the opinion of the guidance of ABA Formal Opinion 92-369, Disposition of Deceased Sole Practitioner's Client Files and Property.

In the ABA opinion sole practitioners are urged to develop a plan for the protection of client interests in the event of their death to include designation of a lawyer to assume responsibility for closing the practice. It identifies two primary duties for the lawyer assuming responsibility for the practice – (1) the duty to inspect files and protect client confidentiality and (2) the duty to maintain client files and property:

The duty to inspect files and protect client confidentiality involves a determination of which files need immediate attention, notification of all clients of the death of their lawyer, and a request for instructions on safekeeping client property. Since the lawyer making the inspection does not represent the clients, care must be taken to review files only to the extent necessary to identify clients and determine matters that require immediate attention. Client confidentiality must be observed to the maximum extent feasible while protecting the clients' immediate interests.

The duty to maintain client files and property is governed ultimately by a rule of reasonableness. While a lawyer does not have a duty to maintain all client files indefinitely, items that likely belong to the client, original documents, and information which pertains to cases in which the statute of limitations has not expired should be maintained or returned to the client. Particular care is required with the disposition of unclaimed funds in the deceased lawyer's client trust account.

Checklist: *Closing Another Attorney's Office*

The term "Affected Attorney" refers to the attorney whose office is being closed.

1. Check the calendar and active files to determine which items are urgent and/or scheduled for hearings, trials, depositions, court appearances, etc.
2. Contact clients for matters that are urgent or immediately scheduled for hearing, court appearances, or discovery. Obtain permission for reset. (If doing so constitutes a conflict of interest, retain another attorney to take responsibility for obtaining extensions of time and other immediate needs.)
3. Contact courts and opposing counsel for files that require discovery or court appearances immediately. Obtain resets of hearings or extensions where necessary. Confirm extensions and resets in writing.
4. Open and review all unopened mail. Review all mail that is not filed and match it to the appropriate files.
5. Look for an office procedures manual. Determine if there is a way to get a list of clients with active files.
6. Send clients who have active files a letter explaining that the law office is being closed and instructing them to retain a new attorney and to pick up the open file. Provide clients with a date by which they should pick up copies of their files. Inform clients that new counsel should be chosen immediately.

7. For cases before administrative bodies and courts, obtain permission from the clients to submit a Motion and Order to withdraw the Affected Attorney as attorney of record. Review SCR 3.130 (1.16).
8. In cases where the client is obtaining a new attorney, be certain that a Substitution of Attorney is filed.
9. Pick an appropriate date and check to see if all cases have either a motion and order allowing withdrawal of the Affected Attorney or a Substitution of Attorney filed with the court.
10. Make copies of files for clients. Retain the Affected Attorney's original file. All clients should either pick up a copy of their files (and sign a receipt acknowledging that they received it) or sign an authorization for you to release a copy to a new attorney. If the client is picking up a copy of the file and there are original documents in it that the client needs (such as a title to property), return the original documents to the client and keep copies for the Affected Attorney's file.
11. All clients should be advised on where their closed files will be stored, and who they should contact in order to retrieve a closed file.
12. Send the name, address, and phone number of the person who will be retaining the closed files to the Director of the Kentucky Bar Association at 514 W. Main Street, Frankfort, Kentucky 40601-1883.
13. If the Affected Attorney was a sole practitioner, try to arrange for his or her phone number to have a forwarding number. This eliminates the problem created when clients call, get a recording stating that the number is disconnected, and do not know where else to turn for information.
14. Contact the lawyer's professional liability insurer about extended reporting coverage.
15. If you have authorization to handle the Affected Attorney's financial matters, look around the office for checks or funds that have not been deposited. Determine if funds should be deposited or returned to clients. (Some may be for services already rendered.) Get instructions from clients concerning any funds in their trust accounts. These funds should either be returned to the clients or forwarded to their new attorneys. Prepare a final billing statement showing any outstanding fees due, and/or any money in trust. To withdraw money from the Affected Attorney's accounts, you will probably need to be an authorized signer on the accounts, you will need a written agreement, or you will need a limited power of attorney. If this is not obtainable from the Affected Attorney due to death, disability, impairment, or incapacity, you may have to request the Director of the KBA to petition the Supreme Court to take jurisdiction over the practice and the accounts pursuant to SCR 3.395.
16. If you are authorized to do so, handle financial matters, pay business expenses, and liquidate the practice.
17. If your arrangement with the Affected Attorney or estate is that you are to be paid for closing the practice, submit your bill.
18. If your arrangement is to represent the Affected Attorney's clients on their pending cases, obtain each client's consent to represent the client and check for conflicts of interest.

Checklist: *Closing Your Own Office*

1. Finalize as many active files as possible.
2. Write to clients with active files, advising them that you are unable to continue representing them and that they need to retain new counsel. Your letter should inform them of time limitations and time frames important to their cases. The letter should explain how and where they can pick up copies of their files and should give a time deadline for doing this.
3. For cases that have pending court dates, depositions, or hearings, discuss with the clients how to proceed. Where appropriate, request extensions, continuances, and resetting of hearing dates. Send written confirmations of these extensions, continuances, and resets to opposing counsel and to your client.
4. For cases before administrative bodies and courts, obtain the clients' permission to submit a motion and order to withdraw as attorney of record. Review SCR 3.130 (1.16).
5. In cases where the client is obtaining a new attorney, be certain that a Substitution of Attorney is filed.
6. Pick an appropriate date and check to see if all cases either have a Motion and Order allowing your withdrawal as attorney of record or have a Substitution of Attorney filed with the court.
7. Make copies of files for clients. Retain your original files. All clients should either pick up their files (and sign a receipt acknowledging that they received them) or sign an authorization for you to release the files to their new attorneys. If a client is picking up the file, original documents should be returned to the client and copies should be kept in your file.
8. All clients should be told where their closed files will be stored and whom they should contact in order to retrieve them. Obtain all clients' permission to destroy the files after approximately 10 years. Lawyers Mutual recommends that closed files be kept for 10 years or longer. If a closed file is to be stored by another attorney, get the client's permission to allow the attorney to store the file for you and provide the client with the attorney's name, address, and phone number.
9. Send the name, address, and phone number of the person who will be retaining the closed files to the Director of the Kentucky Bar Association at 514 W. Main Street, Frankfort, KY 40601. Also send your name, current address, and phone number.
10. If you are a sole practitioner, ask the telephone company for a new phone number to be given out when your old phone number is called. This eliminates the problem created when clients call your phone number, get a recording stating that the number is disconnected, and do not know where else to turn for information.

Special Considerations When Closing A Practice

1. If the reason for closing a practice is the death of a sole practitioner, planning agreements designating a closing lawyer may become void. It will probably be necessary for the estate's executor to authorize the designated lawyer to close the practice. For this reason, part of the planning process should include making sure

there is a provision in the lawyer's will directing the executor to appoint the designated lawyer to close the practice.

2. If the lawyer closing a practice discovers malpractice or ethics violations, the question arises whether this should be reported to clients. The answer turns on whether the lawyer is representing the departed lawyer or is acting in some other capacity.
3. Clients of the departed lawyer may ask the closing lawyer to take over the matter. This is usually permissible provided there is no solicitation by the closing lawyer, the clients understand that the closing lawyer does not currently represent them, clients understand that they may change to any other lawyer they wish, and that the closing lawyer has no conflicts of interest as a result of accepting the matter.
4. Sudden departures sometimes involve a failed lawyer. This often means malpractice claims will be made. The closing lawyer early in the process must review any professional liability insurance. It may be prudent to put the carrier on notice of the situation and seek assistance in preventing claims.
5. Consideration should be given to purchasing from the professional liability insurer an extended reporting period for malpractice claims. Some policies grant automatic extended reporting periods without additional premium in death and disability situations. For example, Lawyers Mutual's policy provides for an automatic extended reporting period at no additional premium upon the death of an insured lawyer and for disabled lawyers if they were insured with Lawyers Mutual for three consecutive years prior to the current policy.

C. Other Unexpected Incidents: Client Notification Requirements in the Wake of a Disaster[4]

In the event that any client or former client files are damaged or destroyed due to a disaster, attorneys may have an obligation to provide notice to each affected client or former client, as well as advise the client or former client of efforts to reconstruct the client file. The following resources may be helpful in understanding your obligations in this regard:

- The ABA Comm'n on Ethics & Prof'l Responsibility, Formal Op. 482 (2018)
- The ABA article, "Ethical Obligations to clients in the wake of a disaster"
- A template client letter to tailor to your situation

Notice to Client Regarding Risk of Disclosure of Confidential Information

Attorneys must first determine whether notice is required to clients regarding risk of disclosure of confidential or privileged information. Based on the ABA's Opinion, above, attorneys are required to notify the client if there was a risk of disclosure of confidential information as a result of the destruction of the physical file (e.g., a confidential

[4] Adapted from materials developed in the wake of the December 2021 tornadoes. Authored by Sarah McKenna, Chase Cunningham, John Selent, and Joe Tucker (*Dinsmore*) with Courtney Risk (Lawyers Mutual),

document or file was removed from the office in the storm and has not been located such that it may be discovered by a third-party).

Notice to Client Regarding Destruction and Reconstruction of the Client File

Next, attorneys must determine whether notice to clients is required regarding efforts to reconstruct the client file. The ABA's Opinion 482 also outlines the following situations that generally do not require notice to the client regarding reconstruction:

- **Electronic Back-Up:** "A lawyer need not notify either current or former clients about lost documents . . . for which there are electronic copies." (Formal Op. 482 at 9.) Thus, when a physical file is destroyed but the file was stored via an off-site electronic restorable backup and can be fully restored, notice regarding reconstruction is not required.
- **Ability to Reconstruct:** If an attorney is already able to reconstruct files from other sources, there is no need to notify clients or former clients of the loss, which is effectively already over. (Formal Op. 482 at 9.)
- **No Intrinsic Value:** "A lawyer need not notify either current or former clients about lost documents that have no intrinsic value [or] that serve no useful purpose to the client or former client." (Formal Op. 482 at 9.) Attorneys will have to make this determination on a case-by-case basis, but it is possible that some files will contain nothing other than public records, not otherwise destroyed, and papers that no longer serve any purpose. Under such circumstances, there most likely is no loss to disclose.

Notice to Client Requirements

Once an attorney has determined whether there is a need to advise a current client or former client regarding the destruction of their physical file, the letter to the client must include the following elements:

Notice — It is an attorney's responsibility to "keep the client reasonably informed" of a matter's status. SCR 3.130(1.4). An attorney also must safely maintain any property held for clients or third parties, such as former clients. See SCR 3.130(1.15).

Reconstruction — Furthermore, an attorney must "provide competent representation" and "act with reasonable diligence and promptness in representing a client." SCR 3.130(1.1), 3.130(1.3). In doing so, the attorney must inform the client or former client of the steps being taken to recreate the damaged file.

Disclosure — Finally, it is an attorney's responsibility to protect confidential client information. See SCR 3.130(1.6). The attorney must advise their client of the risk of potential disclosure of confidential information as part of the destruction of the client or former's client file, to the extent applicable. This is likely to be the case if the file has been removed from the office and cannot be located rather than a file that was destroyed by water damage, but remains in the attorney's possession.

D. Other Unexpected Incidents: Communicating with Clients When a Lawyer Departs a Private Firm[5]

Although Questions I.A. and I.B.[6] both relate to communication about the lawyer's departure, they approach the issue from very different perspectives. Question I.A. asks whether a departing lawyer or the firm must communicate with current clients[7] regarding the departure. Although the question is phrased in terms of communication, the underlying issue relates to both communication and continued representation.

When a lawyer leaves a firm,[8] the relationship between the parties will change, but both the departing lawyer and the firm must take reasonable steps to ensure that client interests are protected and that the requirements of RPC 1.16 are satisfied.[9] To that end, each client for whom the departing lawyer currently is responsible, or for whom the lawyer plays a significant role in the firm's delivery of services, must be notified of the departure and of the client's right to determine who will represent him or her in the future. (This is not to suggest that notice must be given to every client for whom a departing lawyer has done any work. Where the departing lawyer's connection with a client is so limited that the client will not be affected by the departure – for example where the departing lawyer's only involvement with a client was to undertake some research at the request of a supervising lawyer—no notice is required).

This duty to notify the client arises from the lawyer's duty to keep the client reasonably informed under SCR 3.130-1.4[10] and the client's right to counsel of his or her own

---

[5] Excerpt from KBA Ethics Opinion E-424. Kentucky Bar Association, March 2005. Available at https://cdn.ymaws.com/www.kybar.org/resource/resmgr/Ethics_Opinions_(Part_2)_/kba_e-424.pdf.

[6] Question I.A.: When a lawyer terminates his or her relationship with a private law firm, must the departing lawyer, or the firm, communicate with current clients regarding the departure? Answer: Yes. See discussion below.
Question I.B. When a lawyer terminates his or her relationship with a private law firm, may the departing lawyer communicate with individuals other than current clients, including former clients and "firm" clients, regarding the departure? Answer: Qualified Yes. See discussion below.

[7] At the time of a break-up, it is very likely that the departing lawyer will view certain current clients as "his," and the firm will regard the same clients as "firm clients." Irrespective of how the departing lawyer or the firm views a particular client, the client is not property and does not "belong" to anyone.

[8] The inquiry assumes that there is a legal relationship between the departing lawyer and the firm – i.e., the departing lawyer is a part of the organization as an employee, partner, shareholder, member or the like. Lawyers who merely share office space do not normally have the same duties as those described in this opinion. Obviously office sharers need to keep their clients informed of the office location, but there is no choice to be made by the client when office sharers part ways because, unlike the firm, office sharers do not have responsibilities for the clients of one another. If, however, office sharers give the appearance of a firm, then the same duties described above may apply. See SCR 3.130 (1.10), cmt. 1. But see, KBA E-396 (1997) and KBA E-311 (1986) describing the ethical problems of such associations.

[9] SCR 3.130 (1.16(d)) provides "(u)pon termination of representation, a lawyer shall take steps to the extent reasonably practicable to protect the client's interests, such as giving reasonable notice to the client, allowing time for employment of other counsel, surrendering papers and property to which the client is entitled and refunding any advance payment of fee that has not been earned." *See also*, Barbara Rea, Breaking Up is Hard to Do, Ky. Bench & Bar 36 (Spring 1996) on the lawyer's responsibility upon termination of the relationship with the client.

[10] SCR 3.130 (1.4) provides:

choosing, as reflected in SCR 3.130-1.16[11] and 5.6.[12] Not only will the departing lawyer have an obligation to make sure that the client is informed about the change, but those who remain with the firm may have obligations as well. As noted by ABA Formal Opinion 99-414 (1999), "firm members remaining, and especially those with supervisory responsibility, have an obligation under the Rules of Professional Conduct,[13] and may have obligations as well under other law, to assure to the extent reasonably practicable that the withdrawal from the firm is accomplished without material adverse effect on any client's interests…." Recognizing this joint responsibility, the ABA Formal Opinion states that notice may come from the departing lawyer, from the firm, or from both. The Committee agrees with the ABA that joint notice is preferable, but recognizes that this is not always practical. The critical point is that the client receives notice from someone associated with the firm and that the notice impartially and fairly provides the information necessary for the client to make an informed decision about future representation.

The Committee has reviewed a number of ethics opinions[14] from other jurisdictions on the subject of the notice's content and method of communication and concluded that the following principles should be followed where notice to current clients is required:

- Notice may be given in-person or in writing. Although in-person communication with current clients is not prohibited under RPC 7.09(1), the Committee believes that all parties will be better served by written notice.[15]
- Communication should not urge the client to terminate his or her relationship with the firm, but may indicate the departing lawyer's willingness and ability to continue to represent the client.[16]
- Communication must clearly state that the client has the right to decide who shall represent him or her in the future – this includes the firm, the departing lawyer or another lawyer.

(a) A lawyer should keep a client reasonably informed about the status of a matter and promptly comply with reasonable requests for information.
(b) A lawyer should explain a matter to the extent reasonably necessary to permit the client to make informed decisions regarding the representation.

[11] SCR-3.130 (1.16), cmt. 4 provides, in part, "[a] client has a right to discharge a lawyer any time, with or without cause, subject to liability for payment of the lawyer's services."

[12] *See* cmt. 1, expressing the view that one of the policy reasons that the rules prohibit restrictions on the right to practice law (non-competes) is that it "limits the freedom of clients to choose a lawyer."

[13] See SCR 3.130 (5.1), which provides in part:

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

[14] Citation omitted.

[15] Citation omitted.

[16] The departing lawyer must be careful to avoid conflicts of interest occasioned by his or her new affiliation. See SCR 3.130 (1.10).

- All communication with clients (whether initiated by the departing lawyer or the firm) should be respectful of the rights and professional abilities of all concerned and should not be disparaging in any way.

The above discussion relates to communications between the departing lawyer, or the firm, and current clients. Question I.B. raises issues with regard to communications with former clients (those for whom the departing lawyer has done significant work in the past), firm clients (those who have been or are represented by other lawyers in the firm, but for whom the departing lawyer has done no work) and others. The duty to communicate under RPC 1.4 would, by its terms, appear to apply only to current clients. Thus a departing lawyer has no obligation to communicate about his or her departure with former clients or with firm clients. On the other hand, the departing lawyer may wish to advise former clients, as well as firm clients with whom the lawyer has had no association and others, of the change in affiliation. In such a case the lawyer must consult Kentucky's advertising rules, contained in SCR 3.130-7.01- 7.50 and SCR 3.130-8.3 (misconduct). Of particular applicability is SCR 3.130-7.09 (direct contact with prospective clients); SCR 3.130-7.15 (communications concerning a lawyer's services); SCR 3.130-7.20 (advertising); and SCR 3.130-8.3 (misconduct).

E. Other Unexpected Incidents: Data Security

What is an Incident Response Plan, and Why Should Your Firm Have One?[17]

It is important for every organization to have an Incident Response Plan (IRP) in place to address potential cybersecurity incidents. Although it is possible to reduce the number of data breaches and other cybersecurity incidents through risk assessments and adhering to security protocols, not all incidents can be prevented. Thus, it is necessary for any organization to develop an IRP that allows it to rapidly detect incidents, minimize loss and destruction, mitigate any weaknesses that were exploited, and restore IT services.

Establishing an incident response capability should include the following actions:

- Creating an incident response policy and plan
- Developing procedures for performing incident handling and reporting
- Setting guidelines for communicating with outside parties regarding incidents
- Selecting a team structure and staffing model
- Establishing relationships and lines of communication between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies)
- Determining what services the incident response team should provide
- Staffing and training the incident response team

[17] Adapted from "Computer Security Incident Handling Guide: Recommendations of the National Institute of Standards and Technology." U.S. Department of Commerce, 2012. Available at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf.

Kentucky lawyers have further impetus to develop an effective IRP. Because access to confidential information relating to the representation of a client is a key component of the practice of law, so too is the duty to safeguard confidential information.

Commentary to SCR 3.130(1.6), a Supreme Court Rule governing a lawyer's duty to preserve client confidences, clarifies that a lawyer has a duty to act competently to preserve confidentiality. In addition, KBA Ethics Opinion E-446 establishes that:

1. An attorney does have an ethical responsibility to implement cybersecurity measures to protect clients' information;
2. An attorney has an ethical responsibility to advise clients about cyberattacks against the law practice and/or breaches of security;
3. An attorney may utilize third parties and/or non-lawyers to plan and implement cybersecurity measures; and
4. An attorney has an ethical responsibility to ensure that law firm employees, as well as third parties employed by, retained by, or associated with the lawyer, comply with the attorney's cybersecurity measures.

Commentary to SCR 3.130(1.6): Acting Competently to Preserve Confidentiality

(14) A lawyer must act competently to safeguard information relating to the representation of a client 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.

(15) 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.

KBA Opinion E-446: Attorney's Ethical Responsibility to Implement Cybersecurity Measures[18]

An attorney's ethical responsibility to implement cybersecurity measures to protect clients' information is founded upon four (4) separate requirements of the Rules as they relate to competence (SCR 1.1(6)); communications (1.4); confidentiality of information (1.6) and safekeeping of client's property (1.15). Paramount among these ethical obligations is the requirement to "… not reveal information relating to the representation of a client unless the client gives informed consent."

The Commission has previously acknowledged that this provision not only applies to traditional paper communications, but it also applies to the use of emails with clients and opposing counsel, as well as the storing of client information 'in the cloud'. Above all, the attorney must use 'reasonable care' to ensure that the client's confidential information is protected, and that the client's property is safeguarded. Comment (8) to ABA Model Rule 1.1 states that for an attorney to maintain the 'requisite knowledge and skill' required by this provision of the Model Rule, the attorney must keep abreast of the changing risks and benefits of relevant technology.

Effective January 1, 2018, the Kentucky Supreme Court similarly revised its "Maintaining Competence" Commentary (6) of SCR 3.130 (1.1) to include "… the benefits and risks associated with relevant technology…." Further, KBA Opinion E-437 makes it clear that Kentucky lawyers should be competent in the use of technology in their law practices. This 'competence requirement' includes the knowledge of traditional cyber defense tools to protect client data. Thus, "(b)ecause the protection of confidentiality is an element of competent lawyering, a lawyer should not use any particular mode of technology to store or transmit confidential information before considering how secure it is, and whether reasonable precautions such as firewalls, encryption, or password protection could make it more secure."

It should be noted that the type of communication with a client, and/or the method of storing a client's data may require different levels of security. "At the beginning of the client-lawyer relationship, the lawyer and the client should discuss what levels of security will be necessary for each electronic communication about client matters. Communications to third parties containing protected client information requires analysis to determine what degree of protection is appropriate. In situations where communication (and any attachments) are sensitive or warrant extra security, additional electronic protection may be required."

[18] Excerpt from KBA Opinion E-446 (Internal Citations Omitted). Kentucky Bar Association, 2018. Available at https://cdn.ymaws.com/www.kybar.org/resource/resmgr/ethics_opinions_(part_2)_/kba_e-446.pdf.

Due to the constant changing of technology, it is impossible to give specific requirements of what constitutes 'reasonable efforts' by an attorney to prevent cybersecurity breaches. What is 'reasonable' depends upon the facts and circumstances taken to prevent access or disclosure of confidential information. Comment 18 to the Model Rules provides some guidance:

> "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)"

By no means, however, is an attorney ethically held to a 'strict liability' standard in efforts to prevent cyber-attacks. Nor do we mandate specific measures or suggested safeguards that an attorney must take to avoid 'hacks' in order to satisfy this ethical responsibility. Instead, this Opinion updates historically held ethics guidelines for keeping client information confidential in light of the ever-changing use of technology in the practice of law.

Furthermore, as an attorney is under a continuing obligation pursuant to SCR 3.130 (1.1) to "… keep abreast of changes in the law and its practice …" so too is the attorney to undertake continuing technology education to increase cyber-preparedness, and to continually reevaluate policies and procedures in place to minimize data breaches of a client's confidential information.

Common Pitfalls in Incident Response Plans[19]

Using the term "breach." An IRP is designed to allow an organization to evaluate and respond to a suspected or actual cyber security *incident*, whether a breach of computer systems, or the theft, loss, or unauthorized disclosure of personal information. Thus, an effective IRP is triggered before an actual data breach is confirmed. What is more, it will cover a broader range of occurrences than "breaches of the security of the system" as that term is used in KRS 365.732(1)(a), a statute which establishes an organization's responsibility for notification of affected persons when a computer security breach occurs. Regulators and plaintiffs' attorneys alike could latch on to any internal references to an incident as a "breach," even when it does not meet that legal definition.

[19] Excerpt from "Incident Response Plan – Why You Need One and How to Create It." Beazley Breach Insights. Available at https://www.beazley.com/documents/Insights/201609-incident-response-plan-why-you-need-one-and-how-to-create-it.pdf.

Using "shall" when you mean "may." Every attorney is familiar with the different treatment courts afford the terms "shall" and "may" in construing statutory and contractual provisions. The same is true when a plaintiff's attorney or regulator reviews an IRP to determine whether your organization followed its own internal processes. Remember that every incident is different, and the IRP should reflect that a one-size-fits-all approach is not necessary or appropriate.

Too long or too short. If the IRP is too long or detailed, members of the IRP Team will be less likely to stay familiar with it and implement it as written. That said, it should be detailed enough to (1) identify all Team members; (2) allow Team members to understand their roles; and (3) clarify how and when to call upon outside resources when necessary.

Omitting paper records. KRS 365.732(1)(a) and other statutes that govern an organization's responsibility to address suspected or actual cyber security incidents apply only to electronic incidents. However, state and federal laws (such as HIPAA) protect paper records, as well. Thus, a robust IRP will cover data regardless of the format in which it is stored.

A business hours IRP. Incidents are guaranteed to be discovered at inconvenient times: evenings, holiday weekends, or while key IRT Team members are out of the office. An effective IRP will include ways to reach IRP Team members 24 hours a day and provide for backups when they are unavailable.

Cyber Security Risk Management[20]

Cyber Security Assessment and Plan

Efforts to protect your law firm from data breaches begin with a law firm discussion on cyber security issues and the development of a plan to detect intrusions, respond to those intrusions, and mitigate their impact with an effective response. Discussion should first focus on an assessment of all cyber security risks associated with the law firm's use of technology, including email communications, e-filings with state and federal courts, the exchange of discovery in litigation, and maintenance and storage of digital client information and files.

1. Have you appropriately assessed all of your law firm's cyber security risks?
2. What steps have been taken to evaluate those risks?
3. In the event of a breach, does your law firm have an effective response plan?
4. Who is responsible for the implementation of the plan?
5. Are employees of the law firm aware of the plan and trained in the role they play?
6. Has the plan been tested to make sure it works?
7. How are communications with clients, the court, and third parties to be handled?
8. Do you have resources to make required notifications by Kentucky law to clients?

[20] Excerpt from "Attorney's Liability for Data Breach." Lawyers Mutual of Kentucky, 2016. Available at http://www.lmick.com/item/attorney-s-liability-for-data-breaches-2.

Evaluate Your Law Firm's Computer Practices

1. Do you have written computer and information system policies and procedures?
2. Do you require employees to follow those policies and procedures?
3. Do you use commercially available firewall protection?
4. Do you use commercially available anti-virus protection?
5. Do you install updates to those protections in a timely manner?
6. Do you have alternative controls to prevent unauthorized access to your systems?
7. Do you have and enforce policies concerning the encryption of internal and external communications?
8. How is the use of portable computers or media devices affected by these policies?

Consider Your Law Firm's Operational Practices

1. How are passwords established, recorded, and updated?
2. When an employee leaves do you terminate all computer access and user accounts, change pass codes and use authorizations?
3. When you obtain a client or a third-party vendor, do you verify security information and privacy controls and then monitor or audit them?
4. When you terminate a client or a third-party vendor, do you terminate its computer access and user accounts, as well as email authorization?
5. What format do you utilize for backing up and storing computer system data?
6. Do you have the competency to evaluate your IT system or is a third party the appropriate entity to make that evaluation?

Cyber Security Liability Insurance

Cyber security liability insurance emerged at the end of the 1990's to cover losses of revenue and data restoration costs from corporation cyber-attacks. It was not until California passed the world's first data breach notification law that demand for commercial coverage for law firms began. Insurers now provide cyber security liability insurance coverage to pay for expenses associated with notification to clients, credit monitoring for the affected clients, IT forensics, public relations fees, defense costs and civil fines from privacy regulation actions, and civil litigation. Some policies also extend coverage to address loss of income as a consequence of the network's downtime and for property damage to the firm's physical assets. Theft of the law firm's own intellectual property, however, remains uninsurable as insurance companies have struggled to understand the intrinsic loss value if the system is compromised.

Tips for Communications with Clients and Media as Part of Incident Response

Whether your firm is facing a cybersecurity-related incident or a succession event such as a partner unexpectedly leaving the firm, you should be prepared to give timely and detailed information to clients and the media to the extent possible. Regardless of the

type of incident in question, an effective communication plan will include the following elements:

1. **A factual description of the incident:** Keep it brief, factual, and focused: "just the facts."
2. **Initial response details:** Identify the "who, what, when, and where." In the early stages of a cybersecurity incident, you may not know the "why." It is important to refrain from speculating as to the "why." Instead, wait until all the facts can be evaluated and confirmed.
3. **A statement of ongoing processes to minimize and respond to the incident:** Identify what process and procedures will remain in place in order to return to "business as usual" scenario. For a law firm, communications relating to a cybersecurity incident may emphasize ongoing security measures and highlight that data backups are in place and/or that attorneys and clients can rely on paper files until system interruptions can be resolved.
4. **A statement of commitment to return to "business as usual":** If the firm's return to business as usual will be delayed or altered, details of those terms must be communicated when they can be confirmed.
5. **An expression of empathy to those affected by the incident:** Particularly if a cybersecurity incident affects clients, the firm should make every effort to show compassion.
6. **Access to subject matter experts for media inquiries:** This is more directly related to cybersecurity incidents than to communications when a key figure such as a partner leaves a firm. When it comes to providing specific information about a cybersecurity incident, leave it to experts who understand the details of the cybersecurity incident at issue and how it relates to operations.
7. **Timing for follow up information:** Refrain from predicting response times, but communicate with clients and the media as to incremental times for situational updates where possible.