Lawyers Mutual
www.lmick.com

The Risk Manager

A quarterly newsletter by Lawyers Mutual Insurance Company of Kentucky

SUMMER 2014
Volume 26, Issue 3

LETTERS OF ENGAGEMENT ARE A HOT TOPIC WITH INSURERS AND RISK MANAGERS

The best evidence of the increased concern over use of letters of engagement (LOE) by lawyers is that two sessions of the recent ABA Spring Legal Malpractice Conference were devoted to that issue. Insurers and risk managers are up in arms over lawyers' inconsistent use and down right neglect of LOEs. The concern centered on legal malpractice liability and stricter underwriting standards — both with premium increase implications. This development suggests that this is a good time to offer an analysis of the issue with some risk management guidance.

Why Don't Lawyers Routinely Use LOEs?

Why They Should!

The ABA Conference and the 2011 Legal Malpractice & Risk Management Conference offered these examples of why many lawyers fail to use LOEs and why they should:

Don't use because:

- My clients will be offended by a lengthy highly detailed LOE. They are too formal and off-putting.
- I don't want to limit my work for this new client.
- She was a long-standing client.
- I was charging very little; this was a favor for a friend; it was just a question at a cocktail party.
- How likely are we to be sued?
- A boring waste of time and anyway the dog ate my LOE for this matter.

Should use because:

- Complies with Rules of Professional Conduct on competence, diligence, client communication, and fees.
- Avoids good faith misunderstandings or miscommunications.
- May generate additional work.
- Good way to cover file retention and destruction.
- Is Exhibit A in the defense of any malpractice claim or bar complaint. It is the first thing the court or bar counsel will want to look at.
- One authority observes cynically "everybody lies." Even if an exaggeration the point is well taken.
- Will reduce conflict risks and settle scope of engagement issues.
- By specifically identifying who is the client, an LOE protects against suits by non-clients.
- Can make the difference between triable issues of fact and summary judgment.

continued on page 2

"Compromise on public issues is the price of civilization, not an abrogation of principle."

Alan Greenspan

continued from page 1

Letters of Engagement

The first risk management action that should be taken with every new matter after a conflict of interest check is the preparation of a comprehensive letter of engagement including fee terms and conditions. Many lawyers confuse a fee agreement with an LOE. A fee agreement standing alone is not an LOE – it accomplishes few of the purposes or protections of a thorough LOE.

The following checklist identifies key considerations in tailoring a comprehensive LOE for a new matter:

1. Client Identification
2. Related-Party Identification
3. Conflict of Interest, Attorney-Client Privilege, and Confidentiality Issues
4. Scope of Representation
5. Related Matters and Limiting the Scope of Representation
6. Identification of Goals
7. Scope of Authority
8. Staffing the Engagement
9. Legal Fees and Expenses
   - retainers
   - rate changes
10. Billing Procedures
    - format
    - the client's responsibilities for fee payment
    - how often the client will be billed
    - when payment is expected to be made
    - the firm's options when fees and costs are not paid timely
    - whether interest will be charged for late fee payment
    - what fees are due if the client discharges the lawyer before completion of the representation
11. Scheduling Major Steps
12. Consent for Use of Email, Smart Phones, Cloud Computing, and Any Other Electronic Device The Firm Uses to Send Client Confidential Information
13. File Retention and Destruction
14. Dispute Resolution
15. Withdrawal or Termination
16. Signature by Lawyer and Client*

** This list is a composite derived from several sources to include Legal Malpractice 2009 Edition, § 2:10 and the Minnesota Lawyers Mutual Insurance Company.*

Sample LOEs are available on Lawyers Mutual's Website at *lmick.com* – click on Resources (*do not click on the drop down menu*) and then on the listed LOEs.

Risk Management Procedures for Implementing LOE Requirements

Many firms have a policy to use LOEs in all representations, but many are also inconsistent in following this policy. At the ABA Conference the following compliance procedures were recommended:

- Cannot open/work/bill a file until conflicts are checked and cleared.
- Cannot open/work/bill a file until an LOE is sent (and returned). After contemplation, send an LOE immediately by mail or email.
- Have approved template letters for each practice group.
- Make sure attorneys AND staff understand the importance of LOEs – audit.
- Countersignature from client required – diaried.
- For existing clients, send email confirming scope of new matter.

At the 2011 Legal Malpractice & Risk Management Conference it was recommended to send LOEs by email because it is easier that way to get acknowledgement and return. Be sure to diary this email procedure to assure that acknowledgment is received and saved. Instruct the client to print the LOE, sign it, and mail it back. Make sure that the signed copy is received.

Should a Lawyer Always Have a Client Countersign an LOE?

Kentucky does not have a rule requiring that clients countersign all LOEs. Kentucky Rule of Professional Conduct 1.5, Fees, (c) does require that a contingency fee agreement be in a writing signed by the client. Therefore, a lawyer must obtain a client's signature on an LOE that includes a contingency fee agreement.

Notwithstanding this limited requirement, good risk management means using an LOE in every matter and having it countersigned by the client. Be leery of sudden emergency matters when the client insists on immediate service without a LOE. The tendency is to not follow up with an LOE when time permits. This can lead to serious misunderstandings between lawyer and client.

continued on page 3

"The problem with growing up is that once you're grown up, people who aren't grown up aren't fun anymore."
Lev Grossman, The Magicians

continued from page 2

Don't Overlook the Other Engagement Letters – "Dis" And "Non"

Space does not permit a detailed analysis of disengagement and non-engagement letters. Our long-standing risk management advice on their use follows:

Disengagement:

Whenever possible withdrawal should be a clean break – a clear-cut decision with the client's agreement in writing. Use a disengagement letter that:

- Confirms that the relationship is ending with a brief description of the reasons for withdrawal.
- Provides reasonable notice before withdrawal is final.
- Avoids imprudent comment on the merits of the case.
- Indicates whether payment is due for fees or expenses.
- Recommends seeking other counsel.
- Explains under what conditions the lawyer will consult with a successor counsel.
- Identifies important deadlines.
- Includes arrangements to transfer client files.
- If appropriate, includes a closing status report.

After sending the disengagement letter, carefully follow through on the duty to take necessary actions to protect the client's interest and comply with the representations in the disengagement letter. This avoids a malpractice claim over the manner of withdrawal.

Finally, a complete copy of the file should be retained. A disengaged client or one that terminated you has a high potential to be a malpractice claimant. The first line of defense is a complete file with a comprehensive disengagement letter. This is the best evidence for showing competent and ethical practice in disengaging a client.

Non-engagement:

Always use letters of non-engagement for declined representations. They are best sent by certified mail, return receipt requested. A former prospective client with a complaint or claim "never" receives a non-engagement letter sent by regular mail. A typical letter:

- Thanks the prospective client for making the personal contact, calling, or coming into the office.
- Includes the date and subject matter of the consultation.
- Provides clearly that representation will not be undertaken.
- Repeats any legal advice or information given — making sure that it complies with the applicable standard of care.
- Advises that there is always a potential for a statute of limitations or notice requirement problem if the matter is not promptly pursued elsewhere. *Providing specific statute of limitations times should be avoided because of the limited information typically received in a preliminary consultation. If, however, it appears that a limitations period will expire in a short period of time, the declined prospective client should be informed of this concern and urged to seek another lawyer immediately.*
- Advises that other legal advice be sought.
- Avoids giving an exact reason for the declination, why the claim lacks merit, or why other parties are not liable.
- Encourages the person to call again.

DON'T LET THE CLOUD RAIN ON YOUR PRACTICE

Cloud computing is the technology that permits law firms through the Internet to access software or store files on computers that are not at the firm's physical location or even within the firm's physical control. As the invention of the Colt .45 was the great equalizer for the little guy in the Wild West, the Cloud is the great equalizer for small law firms to compete with large firms in the technology driven age in which we practice.

We first wrote about Cloud computing in our Summer 2012 Newsletter in the article *What Kentucky Lawyers Need to Know about the Ethics and Risk Management of Cloud Computing.* That article provides an overview of Cloud computing including the benefits of Cloud computing, the risks of using Cloud computing providers, the professional responsibility rules Cloud computing invokes, and reasonable care in selecting a Cloud service provider. That article remains a good place to start in reviewing your use of Cloud computing. It is available on Lawyers Mutual's Website at lmick.com – click on Resources, Subject Index, Internet, and select the article.

Late last year the New York City Bar issued the report *The Cloud and the Small Law Firm: Business, Ethics and*

continued on page 4

"Elegance is the only beauty that never fades."
Audrey Hepburn

continued from page 3

Privilege Considerations. Given the large number of small firms in Kentucky this report could not have come out at a better time. The report describes the significance of Cloud computing for smaller firms as follows:

> By leveraging this new technology, small law firms could afford the tools needed to grow their practices and compete on a level playing field with large law firms. Small firms or solos who previously could not afford physical storage space could now store their numerous client related documents on the Cloud, without having to worry about the cost and feasibility of hiring an IT department. More importantly, through the Cloud and wireless computing, small firms and solo attorneys could have constant access to client documents and communications whether they are travelling, in court, at a coffee shop, or at home. This increased availability to respond to their clients will give small firms an advantage that in the past they may have ceded to big firms with armies of associates and support staff.

The 29-page report includes this scope statement:

> This paper will explore the landscape of what is reasonable care. It will analyze required safeguards for client and firm electronic information in the context of law firm practicalities, and the business case for moving to the Cloud and using portable devices. It will also outline ways in which lawyers should carefully evaluate all service providers to ensure that they employ sufficient procedures to protect clients' confidences and electronic information and how best to employ appropriate precautions when using portable media. Finally, the paper will propose practical ways to mitigate risk as information technology advances. It will offer ways in which lawyers can, and must, become educated regarding the technologies, and it will outline procedures required when contracting with Cloud providers and utilizing portable devices in order to safeguard client and firm data, thereby minimizing ethical and malpractice risks.

The report concludes with these suggested guidelines:

Guideline 1 – Only Use Reliable Providers
Only use reliable providers and, even with well-established providers, keep up to date on their business condition and prospects.

Guideline 2 – Document Due Diligence
Spend time performing due diligence on a proposed provider and its contract (Service Level Agreement, or "SLA") and document the process, including your review, any negotiations with the provider and the reasons why you concluded that your client's information is going to be secure.

Guideline 3 - Read the Contract, then Decide Your Risk Tolerance
Never just click "Agree" to a provider's "Terms and Conditions of Use." Obtain, and review, the complete Service Level Agreement and all Addenda and Attachments. Read all website information referenced in links in the SLA.

Guideline 4 – Key Contractual Terms
Get promises from a prospective Cloud provider, in the SLA, that it will meet your key requirements, and check the provider's track record of meeting them with reliable references.

Guideline 5 - Get Client Consent
Obtain your clients' consent before storing their information in the cloud or relying on cloud-based software for client-critical functions.

Guideline 6 - Understand the Technology
Be sure you know the technology or engage an expert to assist you.

Guideline 7 – Keep Data Encrypted

Guideline 8 – Establish Data Management Policies and Procedures

The New York City Bar report *The Cloud and the Small Law Firm: Business, Ethics and Privilege Considerations* is an outstanding treatment of Cloud computing for any law firm, but especially smaller firms. We recommend that you refer to it extensively in using and risk managing Cloud computing. All you have to do to obtain it is to Google *The Cloud and the Small Law Firm: Business, Ethics and Privilege Considerations.* (last viewed on 6/23/14)

KEEPING UP WITH LAWYER SCAMS

Cryptolocker

Cryptolocker is a ransomware virus threat to lawyer files and wallets. It is estimated that law firms and businesses have lost millions of dollars to this scam. The December 2013 LAWPRO Magazine featuring "Cyber Crime and Law Firms" describes ransomware as follows:

continued on page 5

A good motto for risk managing your firm's website: "You can never be too rich or too thin or have too many disclaimers."
Randy Manilof

continued from page 4

Ransomware infections are becoming much more common recently and are usually spread by infected email attachments or Website links that trigger a download. The most common type, Cryptolocker, will scramble all the data files on your computer with virtually unbreakable encryption. You learn you are infected when a pop-up window tells you that your data has been scrambled and will be deleted unless you pay a ransom within a very short period of time, typically 48 hours or so. The ransom is typically in the range of $100 to $300 and payable only in Bitcoins, a type of virtual currency that makes payments untraceable. It is a relatively low amount so you have an incentive to pay it as a nuisance; but as you are dealing with criminals, paying it does not guarantee that you will get your data back.

A North Carolina firm was victimized earlier this year by Cryptolocker. The firm was targeted using email with an attachment. Upon opening the attachment the virus immediately began encrypting thousands of documents making them inaccessible to the firm. The hackers demanded $300 within three days to provide the code to unlock the files. After trying to solve the problem without success, the firm attempted to pay the ransom but time had time ran out and could not get the release code. Fortunately, the firm had backup systems.

We are unaware of any Kentucky lawyers victimized by Cyberlocker, but the chances are good that there are some. Given the great variety of computer systems used by lawyers we can only give the following general risk management advice gleaned from several sources. For a comprehensive treatment of computer security risk assessments for law firms see *Cybersecurity Standards and Risk Assessments for Law Offices: Weighing the Security Risks and Safeguarding Against Cyber Threats* by David Z. Bodenheimer and Cheryl A. Falvey. Just Google the article title. (last viewed 6/23/14)

Cyber Attack Risk Management Considerations:

- Use computer-security software to block suspicious emails – be sure to update regularly.
- Never open attachments from a source you don't recognize.
- Require all firm members to be especially vigilant before downloading photos or PDF files even if apparently from known sources to avoid downloading an executable file that could download malware.
- Establish off-site data backup systems and procedures for alternate access to the network.
- Back up and archive all files nightly in an off-line system that is not connected to the vulnerable main office system. Some firms nightly back up all files on tape and lock the tapes in a fireproof safe in the office. They then further back up the files in off-site storage– usually in the Cloud.
- Include home computers, laptops, and smart phones in office cyber security programs.
- Review computer system backup architecture and file-sharing architecture to assure that a single event of a malware download cannot infect both the main system and backup systems.

For additional risk management considerations for Cyberlocker and other malware read The LAWPRO Magazine: December 2013 at:

(http://practicepro.ca/lawpromag/LawproMagArchive.asp) (last viewed 6/23/14)

It is an excellent source for reviewing the cyber risks of your firm. It contains useful guidance for protecting your practice from being held up for ransom.

Editor's Note: Federal authorities recently stopped the primary hacker using Cryptolocker, but as the following paragraphs show ransomware remains a major risk.

Ransomware Hits iPhones and iPads in Australia

ABC Internet News reported on May 28, 2014 that a hacker with the name "Oleg Pliss" locked up iPhones and iPads in Australia and sent ransom messages demanding payment to unlock them. Especially alarming is that hackers may now be able get iCloud credentials from these devices and get to data stored or backed up on the Cloud by the device owner.

This new development in cyber crime reinforces the urgency required in establishing risk management procedures that protect firm backup systems from penetration through any office or home computer or electronic device used by a firm for communication.

"When your children are teenagers, it's important to have a dog so that someone in the house is glad to see you." *Nora Ephron*

Lawyers Mutual
www.lmick.com

Waterfront Plaza
323 West Main Street, Suite 600
Louisville, KY 40202

PRESORTED STANDARD
U.S. POSTAGE
PAID
LOUISVILLE, KY
PERMIT NO. 879

Malpractice Avoidance Update
Member National Association of Bar Related Insurance Companies

For more information about Lawyers Mutual, call ***(502) 568-6100*** or KY wats ***1-800-800-6101*** or visit our Website at ***www.lmick.com***

continued from page 5

HAVE YOU COMPLIED WITH SCR 3.175'S NEW REQUIREMENT ON EMAIL ADDRESSES?

A member of the KBA Ethics Committee brought to our attention that apparently many Kentucky lawyers are not aware of the new requirement in SCR 3.175, Efficient enforcement; notice of attorney's address (effective January 1, 2014), to report their email address to the KBA. The rule now requires that KBA members:

> (b) maintain with the Director a valid email address and shall upon change of that address notify the Director within 30 days of the new address, except however, that "Senior Retired Inactive" members and "Disabled Inactive" members shall not be required to maintain an email address;

If you have not managed to comply with this requirement, now is a good time to catch up. To add or change your email address, go to the KBA website and follow this guidance:

- Login and look yourself up in the Lawyer Locator to see the address on file; then
- Login and complete the online address update form or
- Complete and return a PDF of the Address Change form.

CORRECTION

In the Spring 2014 Newsletter the citation for *Abel v. Austin* erroneously transposed page numbers. The correct cite is 411 S.W. 3d 728 (Ky., 2013).