Can an engagement letter protect you from cyber-related liability?

By Bethann R. Lloyd

Beginning with the assumption that all the lawyers in your firm are actually drafting and updating client engagement letters on a regular basis, are you also utilizing your engagement letter to guard against a cyber-related liability claim from your client and minimizing your risk? If not, you are missing a valuable risk management tool.

For those lawyers handling legal malpractice and disciplinary board matters on a routine basis, the benefits of utilizing an engagement letter are widely known. For instance, a well written engagement letter should eliminate doubt as to who the lawyer does (and does not) represent, what services the lawyer is providing (and any limitations), and the terms of payment, to name just a few key items. Client confusion in these areas all too often surfaces in the form of a malpractice or ethics case against the lawyer.

Another common theme arising in a malpractice or ethics case is a breakdown in communications between the lawyer and the client. Although a lack of communication is typically not malpractice in and of itself, a client who feels neglected or uninformed, whether by perception or reality, has a reason to question the legal services provided, harming the relationship and increasing the likelihood of a lawsuit if something goes wrong in the matter.

With the advent of electronic communications and its ever increasing utilization over the past decade as a form of communication between a lawyer and a client, discussing the ground rules for electronic communications upfront, and confirming in an engagement letter or separate document, will not only get your representation off to a good start, but make sure that you are on the same page as your client, guard against any unique risks and thereby minimize the risk of a future claim against your firm.

First, at the outset of any representation, discuss with your client the preferred method of communication. Often, email is the default method used to keep a client timely informed of developments, but not all clients desire to use email. Conversely, some will only communicate utilizing email. Instead of taking it for granted that the client desires use of email to communicate, have the discussion with your client.

Second, if you and your client plan to engage in electronic communications, and most will, discuss with your client whether a particular method of communication poses an unacceptable risk that can or should be avoided. For example, unencrypted email is not as secure as encrypted email, but does involve an extra step on the recipient’s end that perhaps your client might not desire. By communicating to your client that you are aware of cyber threats, take the issue seriously and are willing to adapt to protect the client, you are instilling confidence in your client. And, through this method, both the lawyer and client participate in assessing the risk, guarding against it, and agreeing in advance upon what level of security and specific security measures are appropriate.

No method is foolproof. However, it is a lawyer’s job to assess the risk and protect the client’s confidences. See ABA Comm. on Ethics & Prof’l Responsibility, Formal Opinion 477 (2017).

When communicating with your client about cybersecurity, document that discussion as you would any other form of important advice, from the very outset in your engagement letter. Consider a simple paragraph to be included as follows:

Our lawyers may communicate with you or others by email, facsimile transmission, send data over the Internet, store electronic data via computer software applications hosted remotely on the Internet, or allow access to data through third-party vendors’ secured portals or clouds. Electronic data that is confidential may be transmitted or stored using these methods. In using these data communication and storage methods, our firm makes reasonable efforts to keep such communications and data access secure in accordance with our obligations under applicable laws and professional standards. You recognize and accept that we have no control over the unauthorized interception or breach of communications or data once it has been sent or has been subject to unauthorized access, notwithstanding all reasonable security measures employed by us or our third-party vendors.

In combination with the above clause, or even as a simple stand alone option, consider asking the client in the engagement
letter or otherwise to respond to basic questions with a yes or no answer, such as:

Question 1: Do you authorize us to communicate with you through unencrypted email? Yes or No?

Question 2: Do you have any special concerns in respect to our use of electronic communications or storage of electronic data? Yes or No?

If, as a result of your discussions, the client requires extra protection, or the subject matter in your opinion warrants it, also include in your engagement letter, or a follow up letter, the specific agreed upon steps that you will take to protect such confidences. For example:

We have discussed that certain subjects and/or documents in this case are of a highly sensitive nature and warrant extra protection. We will utilize encryption when communicating electronically with you in relation to the following subjects or when sending documents relating to these subjects . . .

If extra security measures lead to additional expense for the firm, document that also in your engagement letter, in respect to the anticipated cost and who is responsible for payment.

In addition to the above, consider including an additional provision in your engagement letter by which the client agrees that your firm will not be liable in the event of an unauthorized interception. For instance:

We specifically disclaim any liability or responsibility whatsoever for such interception or unintentional disclosure, and you agree we shall have no liability for any loss or damage to any person or entity resulting from the use of email transmissions.

Whether or not the above disclaimer will be deemed legally enforceable as against a future claim by your client is unknowable, but it will provide you with a defense, particularly if you have demonstrated, through documentation either in the engagement letter or by separate written communication, that you have taken reasonable steps to secure the client’s data, that the client participated in the process and approved of the level of risk in an informed way.

If you are already one of the wise attorneys who takes the risk of electronic communication seriously and takes reasonable steps to guard against the risk, why not get credit for your efforts by documenting it in your engagement letter? By memorializing your efforts to protect a client’s confidences, whether in an engagement letter or by separate communication, you will promote a better client relationship and reduce your chances of a claim.

For more information on Professional Liability Insurance contact USI Affinity.

Lloyd is an attorney at Weinheimer, Haber & Coco, P.C.

---

1 Although beyond the scope of this article, certain federal, state or even international laws may require certain levels of security.