THE SHELY FIRM, PC

Ethics Considerations Before Using Technology

Fall, 2015

By Lynda C. Shely

This paper addresses some of the ethical issues faced by lawyers when using technology, including ethical requirements for: storing data electronically (.pdf) and/or remotely ("cloud computing"), using email, dealing with social media use by lawyers, staff, judges, jurors, and clients, and what to do in case of a breach of security. The ethical standards discussed herein focus on the American Bar Association's Model Rules of Professional Conduct ("ERs") as well as references to some state case law and ethics Opinions. Check the Rules in your jurisdiction before proceeding!

1. Ask Client Permission Before Storing Data on The "Cloud"

Lawyers have an ethical obligation to "safeguard" client property, including client documents and files, according to Rule of Professional Conduct 1.15. But storage facilities are expensive and paper document retention can be burdensome. This means that unless a lawyer returns the entire file to a client at the end of a representation (ideally a lawyer will return the entire file to the client at the conclusion of the representation), the lawyer must preserve the entire file until it becomes "abandoned property" according to the Uniform Unclaimed Property Act.

Lawyers also ethically must preserve certain records for their firms, including trust account records. Many liability carriers also have file retention requirements as a term in the legal malpractice policies. Accordingly, lawyers must preserve many documents related to the practice of law and preserve those documents either for several years or indefinitely.

In addition to the cost of storage of paper records, security issues and erosion concerns as well as accessibility issues motivate many lawyers to store documents electronically. By scanning the document or converting it into an electronic record (e.g. Word, .pdf, .tif, or .jpeg). The first ethics issue arises in whether a lawyer may store a document only as electronic data or whether the lawyer must preserve the original paper. Ethics Opinions in various jurisdictions authorize lawyers to maintain documents electronically – as long as the original document does not have some intrinsic value. If there is value in the "paper" document, such as original wills/trusts/stock certificates/settlement agreements, the lawyer either must preserve the paper or assure that the original is given to the client for safekeeping. *See, e.g., Ariz. Op. 07-02 (electronic preservation of documents is permissible with client consent).*

The next ethics consideration involves *where* that electronic data is stored. Up until the last few years, most lawyers stored documents on their computer or their law firm's server, which resided in a closet or room within the firm. In the last few years more vendors are marketing remote storage with documents accessible through the internet. The remote storage option means that the documents/data does not exist just on a physical piece of computer equipment.

2. Actually *Read* the "Service Level Agreement" with the Cloud Provider Before Signing On…Because Lawyers Must Understand the Risks of Using Relevant Technology.

May a lawyer – ethically - store law firm records electronically *and* remotely in the "cloud"? The ABA Opinions do not address cloud computing specifically. ABA Opinion 11-459 only addresses emails and permits electronic communications with clients as long as the lawyer warns the client about the possibility of third-party access. *(practice tip: include this in your engagement letters!).* Remember – if your email is stored remotely on another company's server (Cox, Google, etc.) so that you may access email on your smart phone or laptop, that also is cloud computing.

The American Bar Association recently amended Model Rules of Professional Conduct 1.1 (competence) and 1.6(c) (confidentiality) to require lawyers to take "reasonable steps" to protect electronic confidential information. Comment [8] to Rule 1.1 specifically notes:

> [8] To maintain the requisite knowledge and skill, a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

The Comments added to ER 1.6 to explain what constitutes "reasonable measures" to safeguard client information:

> [18] Paragraph (c) requires a lawyer to act competently to safeguard information relating to the representation of a client against unauthorized access by third parties and 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. 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. Whether a lawyer may be required to take additional steps to safeguard a client's information in order to comply with other law, such as state and federal laws that govern data privacy or that impose notification requirements upon the loss of, or unauthorized access to, electronic information, is beyond the scope of these Rules. For a lawyer's duties when sharing information with nonlawyers outside the lawyer's own firm, see Rule 5.3, Comments [3]-[4].

[19] 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. Whether a lawyer may be required to take additional steps in order to comply with other law, such as state and federal laws that govern data privacy, is beyond the scope of these Rules.

These Comments follow ethics opinions from several states that "approve" of remote storage as long as lawyers take "reasonable steps" to investigate the provider's security measures. *See Iowa Ethics Op. 11-01 (2011), New York State Ethics Op. 842 (2010), North Carolina Ethics Op. 2011-6.*

Here are suggestions lawyers should *consider* before agreeing to any cloud computing services:

1. First, the law firm must ask clients to consent to remote electronic storage of their documents and information. Confirm in the engagement letter that the client understands and agrees that the law firm will only keep electronic copies of everything. *Reminder: Some clients have "heightened security requirements" for such things as national security clearances, that prohibit having their data stored on the cloud. Ask clients before storing data on the cloud.*

2. Check with your malpractice carrier. Most policies do not cover theft or destruction of electronic information but there is "cyber" insurance available.

Confirm whether the carrier covers identity theft costs if client information is misappropriated.

3. Create law firm procedures to address what happens if your servers go down, your office is destroyed, or the vendor's servers are down (confirm that law firm staff understand procedures and have emergency contact information).

4. *Negotiate the terms* – providers such as Clio and Box have been known to modify their terms of service to identify who at their companies may have access to law firm data and how cyber incidents are reported to law firm customers.

5. Confirm that your firm will have constant, uninterrupted access to firm data at all times, and confirm how often the system must be down and for how long for maintenance.

6. Confirm the encryption provided for your data, the security at the physical data center, how they screen *their* employees, and timing of notification for cyber incidents.

7. Confirm how the provider responds to subpoenas for information/data about your firm (hint: do they tell you *before or after* they respond to the subpoena?).

8. Confirm how your firm data will be returned to the firm if the company goes out of business (hint: all providers should explain their escrow procedures) or you fail to pay bills.

9. Get recommendations from lawyers you trust about their cloud providers.

10. Read the SLA. If you do not know what an "SLA" ("service level agreement" with the vendor) is or what should be *in* the agreement, hire someone who understands the technology and can review the agreement.

Remember that lawyers are responsible for taking reasonable steps to assure that all vendors and agents (accountants, bankers, IT companies, cloud providers, storage facilities, copy centers, temporary help) maintain the confidentiality and security of client information. "Reasonable steps" to assure that client information is kept confidential and safeguarded means checking the qualifications of any provider (including outside tech vendors) before jumping onto the cloud.

3. Emails Are Part of the Client "File" and Must Be Preserved.

Email communications pose multiple ethical challenges that lawyers frequently forget. Emails are just another form of written communication for lawyers. They are considered "writings" according to the ABA Model Rules of Professional Conduct, and as such, lawyers should treat them the same way they treat letters and pleadings. The following sets forth some of the basic ethical obligations related to emails.

The ABA Model Rules of Professional Conduct ("ERs"), ER 1.0 contains various definitions, including:

> (n) "Writing" or "written" denotes a tangible or electronic record of a communication or representation, including handwriting, typewriting, printing, photostating, photography, audio or videorecording, and electronic communications. A "signed" writing includes an electronic sound, symbol or process attached to or logically associated with a writing and executed or adopted by a person with the intent to sign the writing.

Practice Tip: Train all firm staff and lawyers to treat emails like letters – including but not limited to PROOFREADING the written communication, assuming that the communication could be viewed by a judge someday, and refraining from casual, partial sentences and conversations in email communications. This reminder holds true for communications on a client matter that is sent to opposing counsel or experts. For instance, no lawyer would write a letter to an opposing counsel on behalf of a client and at the end of the letter say "Hey, I'll see you for drinks at happy hour tonight." If a letter would not include such personal dialog, emails should not either…

In most U.S. jurisdictions, clients own the "file" and are entitled to the entire contents of the file. For instance, Arizona Ethical Rule 1.16 Comment [9] provides:

> [9] Ordinarily, the documents to which the client is entitled, at the close of the representation, include (without limitation) pleadings, legal documents, evidence, discovery, legal research, work product, transcripts, correspondence, drafts, and notes, but not internal practice management memoranda. A lawyer shall not charge a client for the cost of copying any documents unless the client already has received one copy of them.

This means that all law firms must have the ability to store, retrieve and search emails, by client, to provide clients with copies of the emails upon request or termination of the representation. Preserving written communications as part of the client "file" includes preserving email communications with anyone about a client's matter – not just emails to and from the client.

Practice Tip: Include a clause in fee agreements that informs clients that they will receive copies of all emails regarding their matter and that the clients should maintain those copies as part of their client files.

4. Lawyers are required to be "competent in relevant technology"

Seriously. And yes, this topic is mentioned again – intentionally – because it is one of the most common omissions in lawyer training. As noted above, the ABA amended the Comments to ER 1.1, the rule on competence, to remind lawyers that, in addition to staying current on their practice areas, lawyers also have a duty to stay current and competent on relevant technology.
While lawyers are not required *personally* to understand all technology, they are required to at least hire information technology personnel who understand relevant technology – and the firm's obligations to maintain competence and confidentiality.

Lawyers who fail to keep current on in technology can violate the Ethical Rules, get sanctioned by courts, and be sued for malpractice if the failure falls below the standard of care. For instance, in *Communications Network Int'l, Ltd. v. MCI Worldcom Communications Inc.*, Docket Nos. 10-4588 (L), 11-0408 (XAP) (2d. Cir. Jan. 12, 2012) a lawyer's failure to update his email address in the court's electronic case records was held by the court to be "indefensible" and did not excuse his delayed filing of an appeal, which was denied as untimely. *See also In the Matter of Cynthia E. Collie*, Appellate Case No. 2012-213164 (Sup.Ct. S.Car. Oct 17, 2013)(interim suspension for failing to provide the Bar and Court with a current email address that the lawyer reviews and responds to on a regular basis).

Practice Tip: Either understand your jurisdiction's requirements for maintaining current email addresses or hire personnel who will keep lawyer email addresses current.

5. ASK clients before emailing them.

Contrary to the common misperception that only "privileged" information is "confidential," under the Ethical Rules ALL INFORMATION about the representation is "confidential" and lawyers have a mandatory duty to preserve that confidentiality. ER 1.6 explains:

> (a) A lawyer shall not reveal information relating to the representation of a client unless the client gives informed consent, the disclosure is impliedly authorized in order to carry out the representation or the disclosure is permitted by paragraph (b).

The ABA Ethics Committee issued Opinion 11-459, which expressly noted that lawyers must warn clients to avoid communicating with the firm using public computers (such as in hotels or libraries) and to use an email address for which only the client is authorized to view the emails. This means reminding clients to avoid using work email addresses or an address for which a soon-to-be ex-spouse has the password.

Practice Tip: Include a clause in all engagement letters/fee agreements that informs clients the firm may communicate with them by email and will use the email addresses the clients provide, and remind clients to use addresses that only they are authorized to view in order to maintain both attorney/client privilege and confidentiality.

> *Sample:* Data Retention and Communication. During the course of the representation, I will provide to you copies of all *substantive* documents (either electronic or paper) that I receive or generate on your behalf, other than documents that you send to me - please only send me copies of documents. **Keep the documents that I send to you (either as attachments to emails or paper)** as they are being tendered to you as your copy of your file**.** Please keep copies of all emails sent to or received from me, as they are part of your file. Thus, you will have a complete file at all times. If you prefer to not communicate by email, please notify me *now*. If you require any heightened security measures for the storage or transmission of electronic data, such as for government clearances, please notify me *immediately*.
>
> At the conclusion of the representation I will return to you any original documents that you provided to me and confirm that you have a complete file. I will retain my copy of your file (which may be retained in electronic format only, stored on a secure remote server accessed via the internet) for three years, at which time it will be destroyed without further notice.

6. **Do not respond to negative online reviews with any information about the representation!**

Former clients sometimes post negative reviews about lawyers on such online sites as YELP, Avvo, Google, and others. While the client may disclose information about a prior representation – and a former client might even *lie* about what the lawyer did or didn't do, a lawyer *cannot disclose information on social media sites to defend herself/himself.*

"Social media," according to several ethics opinions and discipline cases is not a venue that falls within the exception in ER 1.6 that permits disclosures to assert or defend a claim involving a client. ER 1.6(d)(4) permits disclosures:

(4) to establish a claim or defense on behalf of the lawyer in a controversy between the lawyer and the client, to establish a defense to a criminal charge or civil claim against the lawyer based upon conduct in which the client was involved, or to respond to allegations in any proceeding concerning the lawyer's representation of the client;

See N.Y. State Op. 1032 (10/30/14); Pa. Op. 2014-200 (2014); San Francisco Op. 2014-1 (2014); *In re Skinner* , 740 S.E.2d 171, 2014 BL 137684(Ga. 2014) (public reprimand); *In re Tsamis*, Comm'n File No. 2013PR00095 (Ill. 2013) (reprimand); *In re Quillinan*, 20 DB Rptr. 288 (Or. 2006) (90-day suspension);*Office of Lawyer Regulation v. Peshek*, 798 N.W.2d 879 (Wis. 2011) (60-day suspension for posting information about clients on a blog).

7. Stop Putting Privilege Disclaimers at the *Bottom* of Emails.

Really; this is not rocket science. People put disclaimers at the bottom of email messages so that they don't "clutter" the important part of the message. However, if an email only states that the communication is "*attorney/client privileged, work product, and confidential"* at the BOTTOM of the message, there is a very good chance that a misdirected email sent to opposing counsel, instead of to your client, will be read in its entirety before the receiving lawyer even has a chance to be alerted to its misdirection.

While everyone knows these disclaimers actually are not enforceable protection (because you use them on all emails, even those you intend to send to opposing counsel), but they do provide at least a warning notice to the recipient that the information might not be intended for them – if they appear at the top of a message.

Arizona Ethical Rule 4.4(b) provides the following requirements on what to do if you receive something that appears to be misdirected:

(b) A lawyer who receives a document or electronically stored information and knows or reasonably should know that the document or electronically stored information was inadvertently sent shall promptly notify the sender and preserve the status quo for a reasonable period of time in order to permit the sender to take protective measures.

The ABA Model Rule requires that a recipient of something sent "inadvertently" stop reading and notify the sender. How do you comply with this and *not* read an entire email, if the warning is at the *bottom?*

8. **Maintain "professionalism" at all times in all communications means reminding lawyers and staff that email communications must be professional in tone and content.**

Unfortunately, there are many examples of lawyers engaging in less than *professional* vocabulary and comments in email communications – both internal and external. The Florida Supreme Court recently disciplined two lawyers for their inappropriate email exchanges; according to the *ABA Journal* article and the *St. Petersburg Times.* Mr. Mooney received a public reprimand and was ordered to take a class on professionalism and Mr. Mitchell was suspended for 10 days and ordered to attend an anger management class.

Here is another legal news headline that no firm wants to have in the *ABA Journal:*

> *"'Churn that bill, baby!' email surfaces in fee dispute with DLA Piper"*
>
> *Posted* Mar 25, 2013 2:54 PM CST, by Martha Neil, *ABA Journal*

The quote is from an internal email between lawyers at DLA Piper that was produced when the firm sued a client for fees. The firm's explanation of the email communications was, "the emails were in fact an offensive and inexcusable effort at humor, but in no way reflect actual excessive billing." DLA Piper, a well-respected large firm, now has to take the time to deal with negative press over comments that presumably were meant only to be viewed internally and intended to be funny … and those "internal" communications became very public when the firm decided to sue for the fees owed by the client.

Lawyers are human. Lawyers are permitted to get angry, have a sense of humor, or think hostile thoughts towards others … but lawyers and staff must remember that those thoughts should not appear in any writing … including emails.

9. **The Internet Can Be Seen by *Everyone*….*Forever*….So Have Policies**

Ethical Rule 1.6, regarding confidentiality, applies to the internet…and so do all of the other Rules of Professional Conduct. Consider the following cautions before disclosing any client-related information on the internet:

- Seek client permission before announcing successful court decisions or transactions on firm websites, blogs, listservs, or microblogs – *even if it pertains to a reported decision*

- Do not post "hypotheticals" on listservs asking for advice about "a client with two kids in elementary school married to a doctor who needs help with whether she can switch treating doctors without changing a court order when one of the kids has lupus." That is way too much specific information that could be identified by THE OPPOSING COUNSEL who may be on the same listserv… and this includes listservs for commercial litigation and even SEC representations.

- Do not post notices on the firm website or Twitter or LinkedIn of "winning dismissal on technicality on six sexual harassment claims against CEO of major manufacturer" without obtaining client consent. It is NOT privileged information but it absolutely is still CONFIDENTIAL under the Rules of Professional Conduct and cannot be used for a lawyer's own marketing purposes. Not to mention that such posts may alert opposing counsel that an appeal might be advisable if they find out how weak your underlying defense is….This is both a client relations nightmare with the client and a violation of confidentiality.

10. Create and Review Annually the Firm's Social Media and BYOD Policies

Law firm employees are *not* authorized by any law to post comments about clients or to disclose information "relating to representation" of a client. Federal and state labor laws do *not* authorize violations of Ethical Rule 1.6. This requires explaining to employees what information is "related to representation" of a client because many lawyers incorrectly assume they can post comments about a client as long as the information was disclosed in open court. That is WRONG.

Have a Firm Social Media Policy that at least discusses:

- Prohibit staff, lawyers, and vendors (consultants, expert witnesses) from posting any information about clients on their *personal social media sites*, their own websites, or anywhere. Example of a paralegal's "status" line on her personal Facebook,

  "What a Bad Day – client lied in court…."

  Even though she didn't identify the client by name, the client was not happy, and the terminated paralegal had to learn the hard way that this information is CONFIDENTIAL and resulted in sanctions against the client and the firm.

- Do not "write" on a client's Facebook wall or "comment" on something they wrote unless you understand that opposing counsel may read it and the communication is not privileged or confidential…and warn clients about the same concern so *they* don't communicate with firm lawyers or staff informally on Facebook. Better yet, do not "friend" clients…

- Posting comments about a case, client, opposing counsel or judge using a fictitious name does not avoid the ethics violation. And by the way – someone always finds out who is the real author….

- Remember to request permission from a judge before "tweeting" from court because such broadcasts may violate the court's Rules on broadcasting court proceedings.

- Alert all staff to the restrictions on advising *clients* to delete information from their social media sites when litigation is reasonably anticipated or already commenced. *See In the Matter of* 69 *Matthew B. Murray*, 2013 WL 5630414, VSB Docket Nos. 11-070-088405 and 11-070-088422 70 (Virginia State Bar Disciplinary Board July 17, 2013)(lawyer suspended five years for instructing client to "clean up" Facebook account after discovery request). Several ethics opinions clarify that a lawyer may advise a client to change privacy settings to restrict access to the social media but everything is subject to applicable laws that would require preservation of information. *See FL. Bar Op. 14-1 (2015); NYCLA Op. 745 (2013); NC Bar Op. 5 (2014); PA Op. 2014-300; Phila. Bar Op. 2014-5*

- Remind lawyers and staff that even if they are not mentioning client matters on their personal internet jaunts, they do represent the firm when they identify that they work at the firm, and need to be mindful of disparaging anyone (clients, judges, opposing counsels) and engaging in any online conduct that could hold the firm in disrepute.

Have a firm BYOD policy so all lawyers and staff who have *any* firm data on a personal device, such as a smart phone, ipad, notebook computer, home computer, home fax machine, home copier (remember – they have memories), or laptop understand what they must do IMMEDIATELY if that device is lost, stolen, or exchanged.

11. Conflicts of Interest Can be Created by Random Online Advice

An attorney-client relationship *may* be formed whenever someone seeks and receives advice from a lawyer….That is a really broad standard, which means, avoid "inadvertent" or "unintentional" clients:

- Do not give legal advice to "anonymous" people online – they are at least prospective clients under ER 1.18 and may be actual clients under ER 1.7….or worse….they could be the opposing *party* intentionally asking you for advice.
- Do not 'friend' witnesses, opposing parties, judicial staff, *jurors* or anyone else involved in your practice….unless you really are friends with the person in the "real" world.

- Do not accept 'friend' requests from people involved in your litigation or transactional practice…unless you really are friends.
- If you are friends with a juror, opposing party, opposing expert, judge, or judicial staff, you must determine if this is a disqualifying conflict of interest for your firm to continue in the case.
- Train all law firm staff to notify lawyers whenever they are "friends" (real or otherwise) with someone who is involved in a litigation matter being handled by the firm.
- Giving "free" advice online to random people also may subject the lawyer and firm to charges of engaging in the unauthorized practice of law. Several states have prosecuted lawyers from *other states* for advising people online, without clarifying that the lawyer was not admitted in the prospective clients' home jurisdiction….usually because the lawyer never *asked* where the prospective client lived. If you really must answer an online question on a website or blog, always always always identify where you are admitted with the word "only" so, for instance, Lynda Shely is "admitted to practice law only in Arizona, the District of Columbia, and Pennsylvania (inactive)."

12. Provide Regular Firm Training and Updates on Internet Scams

Firms must be ever vigilant at new cyber scams. Cyber-attacks, spoofing, hacking, and lots of other bad "things" happen every day to law firms around the globe. Use IT professionals who are reliable and up to date on the ever-changing possible assaults on your firm's data. One recent spoof that caught many lawyers unaware were fake emails that came from email addresses that looked real (i.e. they appeared "real" when just looking at the reply address), and asked you to look at a document your contact was sending you through Dropbox. However, it was a not a Dropbox link. Everything about the emails look real. DON'T CLICK ON LINKS THAT YOU WEREN'T EXPECTING TO RECEIVE.

Not only did several lawyers' email addresses get "spoofed" (Spoofing: "also known as **IP** address forgery or a host file hijack, is a hijacking technique in which a cracker masquerades as a trusted host to conceal his identity, **spoof** a **Web** site, hijack browsers, or gain access to a network."), but the hijack caused several *other* firms who received the fake emails to have their systems crash simply because of the deluge of data – they didn't even click on the fake Dropbox link!

13. Encrypt Laptop/Notepad Hard Drives And Restrict Work Access to Outside Email Systems

This is almost too basic to discuss with law firms, except lawyers routinely ignore basic data hygiene – to avoid getting sick, take precautions. The most basic of which are: encrypt data, use appropriate internet security systems and software – including keeping them current ("patches" must be installed regularly), know where your firm data is stored (literally), and be vigilant about possible intrusions/misappropriations.

The most common path for invasion into a law firm's digital information is through an employee accessing their personal email account on a work computer. When employees at law firms on their lunch break sit at their work computers and access "AOL" or "Gmail" or other outside vendor sites and then click on emails that appear to be from friends or family, they risk your clients' data being stolen. Law firms are increasing their vigilance at monitoring websites that employees access on firm-owned systems, in order to prevent such cyber thefts and/or viruses. Law firms also frequently restrict use of firm computer usb ports, so infected jump/thumb drives cannot be inserted into firm computers. Talk to your IT personnel about implementing basic electronic data security measures to reduce the risk of inadvertent infection and/or theft of data.

14. Don't Lie – Anywhere. Pretexting and Dissembling May be Prohibited – ER 4.1 and ER 8.4

Ethics standards are pretty easy – tell the truth – all of the time – including online.

Sounds easy and there actually are at least two Rules that require not just candor in court (ER 3.3(a)) but truthfulness in statements to *anyone*: ER 4.1 and ER 8.4.

Note that these truthfulness requirements apply to staff and agents of a lawyer (such as private investigators). This means staff and investigators cannot lie about either their identity or why they are contacting someone online. *Philadelphia Bar Association Opinion 2009-02. See Opinion 843 (9/10/10) of the New York State Bar Assn and New York City's Bar Committee on Professional Ethics Op. 2010-2.*

Staff cannot pretend to "friend" someone because they are a long-lost high school pal when in fact the person is an opposing party and your firm is trying to investigate them.

While Arizona has Ariz. Op. 99-11, which does permit pretexting in very limited circumstances for investigating civil rights cases, no one should rely on this Opinion for justifying pretexting in other contexts.

Note that several other jurisdictions have held that *deleted* FACEBOOK and other social media sites are discoverable in litigation – this means warn your clients to not discuss the litigation or their personal situation on the internet – it will be discoverable.

15. Know Your Reporting Obligations if a Cyber Incident Occurs -Create, review and use a data breach policy

Law firms must comply with data security requirements imposed by clients, federal & state regulations. Almost all U.S. states, including Arizona, require that vendors notify customers/clients of any data security breach that includes "personally identifiable information" – and what constitutes "personally identifiable information" varies state to state. This is not just *HIPAA protected information.* You may be required to report a cyber incident that accesses client names, addresses, social security numbers, or bank account numbers. Note that in 2015 a survey of the 100 largest law firms in the U.S. found that 1 in 4 lawyers

Whether a law firm must *report* a cyber incident depends upon: the size of the firm, the amount of information "potentially" compromised, the type of information, and the states affected.

In addition to state reporting requirements (not just to your clients, but also to state officials), many federal laws have cyber incident reporting requirements, including the Securities and Exchange Commission and the Department of Defense.

A "data incident" includes not just hacking but loss of a cell phone/laptop/ipad that includes such information, returning a cell phone to a carrier in exchange for a new phone, and even loss of a backup hard drive. Whenever a firm loses control over data, that can be a reportable incident under federal and state laws. Not to mention loss of control over information about law firm clients could violate ER 1.6 and may require providing identity theft protection for clients.

Have procedures in writing, review the procedures, and remind all employees of the need to secure client data and notify the firm in the event of any incident.

16. Prepare for the Unexpected

Who knows your password to PACER? Who knows what personal electronic devices you own that have firm information on them – and *where are* those devices? Who knows what websites (seriously – some firm lawyers have separate websites for specific practice areas)/blogs/listservs/chat rooms/email subscription services you use or are responsible for hosting? Sole practitioners have an affirmative ethical obligation to assure that someone responsible has such emergency information in the event of their sudden death or inability to practice law (either permanently or temporarily). Large firm lawyers *also* have the same obligations, which may be satisfied by simply alerting your legal assistant or administrator to your electronic passwords (related to your practice) and presence, the location of information about your pending matters (and how to access that information), and which lawyer(s) have agreed to assist with transferring client matters when you are no longer able to practice law. Do this today. And keep the information updated as you change passwords. And notify the person responsible for your personal estate how to communicate with the designated assisting lawyers.

****

Lynda C. Shely, of The Shely Firm, PC, Scottsdale, Arizona, provides ethics and risk management advice to law firms. She also assists lawyers in responding to initial Bar charges, performs law office management reviews, trains law firm staff in ethics requirements, and advises on a variety of ethics topics including ancillary business ventures, conflicts of interest, fees and billing requirements, trust account procedures, multi-jurisdictional practice requirements, and law firm advertising/marketing. Lynda serves as an expert witness on professional responsibility issues and frequently presents continuing legal education programs around the country. Prior to opening her own firm, she was the Director of Lawyer Ethics for the State Bar of Arizona for ten years. Prior to moving to Arizona, Lynda was an intellectual property associate with Morgan, Lewis & Bockius in Washington, DC. Lynda received her BA from Franklin & Marshall College in Lancaster, PA and her JD from The Catholic University in Washington, DC.

Lynda was selected as the State Bar of Arizona Member of the Year in 2007 and has received other awards from the State Bar for her contributions to Law Related Education Projects and Outstanding Leadership in Continuing Legal Education. Lynda received the Scottsdale Bar Association's 2010 Award of Excellence. She is a prior chair of the ABA Standing Committee on Client Protection and a past member of the ABA's Professionalism Committee and Center for Professional Responsibility Conference Planning Committee. Lynda is the 2015-2016 President of the Association of Professional Responsibility Lawyers and serves on the ABA Center for Professional Responsibility Coordinating Council. She serves on several State Bar of Arizona Committees and has taught ethics at all three Arizona law schools.