Use of Technology to Protect Client Confidentiality

July 2018

Richard A. Mann
Mann Law, P.C.
3750 Kentucky Avenue
Indianapolis, IN 46221
ph: (317) 388-5600 Ext. 211
fax: (317) 388-5622
e-mail: rmann@mannlaw.us

Rule 1.6 (a) A lawyer shall not reveal information relating to 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). In the comments to this rule it is further clarified about your duties.

Acting Competently to Preserve Confidentiality

[16] 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.

[17] 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.

This is where Rule 1.1 comes in.

Rule 1.1. Competence

A lawyer shall provide competent representation to a client. Competent representation requires the legal knowledge, skill, thoroughness and preparation reasonably necessary for the representation.

Within Rule 1.1 now includes competency on technology. This requirement is found under the comments

Maintaining Competence

[6] 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 the technology relevant

to the lawyer's practice, engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject.

I will now discuss the serval ways you can comply with the above rules.

- Inspecting documents in Word You may know that when you use Microsoft Products it has hidden data or metadata in the document. For example, you have an associate or paralegal draft a document for you and then you review it and make changes and or comments about the document and how your client wants to avoid certain issues, so they need to delete or add language. You then send it to your client to review and they make comments. Once you get it back you shut off track changes and then you e-mail the document to the other side as they want it is word. Unless you inspect the document and remove the metadata the other party can see all your comments and your client communication, work product and the like.
- **Office 365 E version:** Restricting e-mails so they cannot be forwarded and can only be accessed using the e-mail it was sent to. If you have Office 365 which seems the way many people are going you can get a version that will encrypt e-mails for you. How many times have you gotten an e-mail from an opposing party who is responding to there attorney where the attorney just forwarded your e-mail. I do not forward the other attorney's e-mail and I make it clear on sensitive things even discovery that they are to return it to me and not the other side.
    - Drop Box At our office we used to use Dropbox to share things within the firm and with clients and co-counsel. While technology saves a lot of time you must understand the dangers of the products. For example, my paralegal's name is Molly and if I want to share a dropbox file with her I started typing her name and to make it easier for me dropbox auto fills her e-mail address. Unfortunately, Dropbox must pull from my contacts in Outlook as there is an attorney named Molly whose name it also tries to add. See JWP Zack, Inc. v. Hoosier Energy Rural Elec. Co-op., Inc., 709 N.E.2d 336 (Ind. Ct. App. 1999): attorney for party inadvertently disclosed documents in production of documents response. Court adopted balancing test to determine if the privilege has been waived:
        - Considering extensive request for production and precautions taken by counsel were reasonable
        - Counsel attempted to rectify the production quickly
        - The amount of documents which were privileged compared to the total amount produced were very small
        - The disclosure was only to 1 person who was not permitted to take the privileged documents from the attorney's office
        - The documents were created for the purpose of the lawsuit and many admonished the reader against disclosure to outsiders

- **Emailing documents to clients:** As I mentioned in Dropbox, Microsoft has what it calls AutoComplete. On my computers I have that turned off as you can accidently e-mail things to the wrong person. For example, my IT guy is Steve Smith of SBSIndy. There

is also in Marion County a bailiff in Probate court whose name is Steve Smith. Both of their e-mail addresses start with steve. For some reason even though I regularly e-mail my IT guy and not the bailiff, if I have AutoComplete on it tries to send the message to the bailiff and not my IT guy. AutoComplete is the default. So, each time I get a new version of Outlook I must go in and shut it off. Another way if you to not want to shut it off completely you can remove the bailiff example one at a time. You can find all the instructions here https://support.microsoft.com/en-us/help/2199226

- **Portal:** Many practice management programs now come with a portal. For example, I use Amicus Attorney Premium. It has a portal whereby I can give my clients access to various things on my system. The access is limited to the things I chose for them to see. For example, if I put a court date on a calendar, I can mark it to be accessible by the portal and then my client can log in and they can see the court date. I can give them access to documents to review and add to them such as discovery responses. We can send each other messages. My clients cannot change my document but when they save a document and do not change the name Amicus does that for them. The portal uses 256-bit encryption. By using portals you may avoid waiving privilege and confidentiality. Emailing clients information could result in them waiving confidentiality or privilege. At our firm we do not use our client's employee e-mail addresses and if they do not have a person e-mail then we do not use e-mail for communications due to the issue of waiving e-mail.
- Use of Facebook as a website: If you use Facebook Messenger, the default is to allow Facebook to read your messages. You should either not use this method or make sure you change the default to encrypted. These messages are different than posts that are like say happy birthday to someone. For other issues on ethical challenges an excellent article appears in the Touro Law Review.
- Emphasizing to your client the need for not sharing information:
- Client postings The US District Court for the Northern District of California ruled in Lenz v. Universal Music Corp., 2010 WL 4 Client postings
    - The US District Court for the Northern District of California ruled in Lenz v. Universal Music Corp., 2010 WL 4780900 (N.D.Cal. Nov. 17, 2010) that the client's postings on social media chats with friends, blog postings, and emails to friends discussing the attorney-client communications was sufficient to waive the privilege and, therefore, the court required the attorney to provide those communications.
  - Client uses work email address
    - Company computer and email address, not privileged and if valid business reason employer can access
    - Often employee handbook includes that employer has right to review
  - Cloud data
    - Must take reasonable steps to ensure safeguards for security: password protect, encryption
    - Harleysville Insurance Co. v. Holding Funeral Home (W.D. Va. 2017): Plaintiff's counsel shared information using direct links to a third party; then party shared information with counsel on same link; 9discovery for third party's file led to defense counsel obtaining the

email with the link; defense counsel used the link to download documents
- No reasonable precautions to prevent disclosure – had used the link to share information with third party prior to using same link to share communications to attorney
- Attorney used same link so was aware for months that this information was on that link and should have known third party access
- Without a password so anyone with access to the link could see the files

- 780900 (N.D.Cal. Nov. 17, 2010) that the client's postings on social media chats with friends, blog postings, and emails to friends discussing the attorney-client communications was sufficient to waive the privilege and, therefore, the court required the attorney to provide those communications.

- **Client uses work email address**
  - Company computer and email address not privileged and if valid business reason employer can access
  - Often employee handbook includes that employer has right to review

- Employees do not have an expectation of privacy in their company e-mail or e-mail accessed on a company device. See Smyth v. Pillsbury Co., 914 F. Supp. 97 - Dist. Court, ED Pennsylvania 1996. In this case, the court found no reasonable expectation of privacy in company e-mail even though the company had a policy claiming it would be confidential.
- In another case of Stengart v. Loving Care Agency Inc LCA, the court carved out an exception when the employee was suing the employer and obtained the e-mails to her counsel in the pending case. The court found in this circumstance the attorney representing the employer should have sought assistance from the court.
  -
- Cloud data
  - Must take reasonable steps to ensure safeguards for security: password protect, encryption
  - Harleysville Insurance Co. v. Holding Funeral Home (W.D. Va. 2017): Plaintiff's counsel shared information using direct links to a third party; then party shared information with counsel on same link; discovery for third party's file led to defense counsel obtaining the email with the link; defense counsel used the link to download documents
    - No reasonable precautions to prevent disclosure – had used the link to share information with third party prior to using same link to share communications to attorney
    - Attorney used same link so was aware for months that this information was on that link and should have known third party access
    - Without a password so anyone with access to the link could see the files

- Case law of attorney-client privilege

- Using Social Media: For a discussion and citations click on link for what you as an attorney should or should not do. Also an article on Social Media as evidence in Indiana and what you should tell your clients.

Alexa, Apple, Microsoft versions: If you have one of the new gadgets, should you have them in your office or anywhere you meet or discuss your clients' cases? If you do you should go in and delete everything on it and give it away. While many people think the thing only listens if you say the code word, it has to be listening at all times to hear the code word. There is now the famous murder case where the police was trying to access the information from Amazon. Or the device sending out random conversations. Should you turn off your cell phone when discussing client information. I recently met with an attorney who was asking for my help on a divorce case. During that talk we mentioned a time share several times. The next day I received numerous emails the next day about time shares. I had never received on before. Do you believe in coincides? Even if you do not want to turn off you phone as many times it is the only way your family can reach you consider turning off the listening mode. https://www.itproportal.com/2015/09/02/how-to-turn-off-ok-google-voice-search/ for a way to do so on Google based cell phones.

- Shut off Cortana listening check your settings on your devices. I recently went through my tablet and I was amazed at all the information that was being taken by default.
- Do not use Automatic Download by apps you have heard of Cambridge Analytica
- Have you ever had you phone ask you to rate a place you are currently sitting?
- Bluetooth issues my tablet has an automatic connection does yours? Is it shut off? How about your telephone?
- LinkedIn. Stop before you click. LinkedIn almost every time I login with my cell phone it tries to upload my contacts to LinkedIn. My Samsung tries to exchange info with others. Not only could you disclose client information you might also be contacting the opposing party who is represented by counsel.
- Is your home and office Wi-Fi secure? Did you know if you have Comcast Xfinity they add a hotspot on your router and it can log you or others into such automatically? If you have a guest Wi-Fi connection is it outside of your server or work computers? At my office we have 2 and only one can log into the computers the other just gives you access to the internet. Both are password protected.
- Do you want the local reporter ringing your doorbell and asking you on camera about your client's records being accessed online?
- Do you tape over the camera on your computer? Do you realize if someone can hack your camera, which I am told is easy, they can still hear your microphone? On my desktop I have a camera with microphone that I keep unplugged except when I am on a video conference.
- One of the default settings in Windows 10 is to automatically allow wireless access to your computer

- Easy password my tablet will unlock if my cell phone is close to it. So if I lose my cell phone and tablet they can open it or they steal it.
- Do you offer wifi at your office? Does it give you access to your server or computers?

Backup backup backup and make sure the they are not over each other

Prepared by Richard Mann of Mann Law, P.C. Attorneys at Law, www.rmannlawoffice.com
Follow us on Facebook: https://www.facebook.com/RAMattorneys?ref=hl
Follow us on Twitter: https://twitter.com/RAMattorneys
Follow our blog: http://ramlawoffice.blogspot.com/
Follow us on LinkedIn: https://www.linkedin.com/in/richardmannfamilylawattorney/

VPN

Do not allow other computers to access yours

Change your settings to clear history when exiting

Do not store history default on IE is 20 days

In IE you can set it to clear your temporary files upon exiting otherwise they are saved to the hard drive

Skype keeps a copy of all your conversations on your computer and can later be retrieved

What happens when you browse privately

- Chrome won't save your browsing history, cookies and site data, or information entered in forms.
- Files you download and bookmarks you create will be kept.
- Your activity isn't hidden from websites you visit, your employer or school, or your internet service provider.

Learn more about how private browsing works. Y

our activity might still be visible

Incognito mode stops Chrome from saving your browsing activity.

Your activity might still be visible to:

- **Websites you visit**, including the ads and resources used on those sites
- **Your employer, school**, or whoever runs the network you're using
- **Your internet service provider**

If you sign in to an account to use a web service, like Gmail, your browsing activity might be saved on sites that recognize that account.

Facebook has everything I have done since 2009 when I was put on it. Including all calls and Every search I have ever run on it in total 60MB and Googe was 50MB

The photos on my telephone end up on my Amazon tv