How to Prioritize Attorney Client Confidentiality at Your Firm

Written by Teresa Matich

It's important to be diligent when it comes to attorney-client confidentiality. Even if you don't outwardly share client information, you could still find yourself in hot water. For example, in April 2016, a lawsuit was filed claiming one Chicago-based law firm had failed to protect confidential client information.

The suit didn't accuse lawyers at the firm of inadvertently sharing client information. In fact, according toThe American Lawyer, "[t]he complaint makes no claim that data was stolen or used against clients." The claim solely focuses on the fact that lax data security could have put client information at risk.

In other words, all firms should prioritize proper precautions for attorney-client confidentiality. However, adhering to these rules is anything but basic, especially in the modern era. Read on to learn more about attorney-client confidentiality and our tips for keeping your law firm secure.

What is the rule of client confidentiality?

ABA's Rule 1.6 Confidentiality of Information speaks to attorney-client confidentiality by stating This Rule governs the disclosure by a lawyer of information relating to the representation of a client during the lawyer's representation of the client. Though, as you read on, you'll find that putting this into practice during the digital era we live in requires diligence and structure from firms and legal professionals alike.

Defining attorney-client confidentiality

Attorney-client confidentiality is one of the longest-running recognized privileges within the American legal system. It "encourage[s] full and frank communication between attorneys and their clients." The idea behind it is, if you cannot tell your attorney all the details about your various legal issues, you may not be able to get full, diligent representation.

This can be a problem. If you watch the innumerable lawyer TV shows out there, this almost always happens—a client is embarrassed about some fact, doesn't tell you about it, and then you have to adjust. It's the standard plot trope.

Fortunately, in the real world, we have attorney-client privilege to help us encourage clients to be honest with their lawyers. But there are some limitations you should know about.

Steps lawyers need to take when it comes to attorney-client confidentiality

Does this mean you need to stop using social media? No. But you do need to reconcile the norm of sharing information online with the need to keep client information confidential.

Below are a few things you can do to ensure you're protecting client information:

- Go private on Facebook. This is a simple step for all lawyers (and for anyone using Facebook, for that matter). Go to "Settings," then "Privacy," and set all of the visibility options so that only "Friends" can see your profile. If you want to market your law firm on Facebook,set up a separate Facebook page—and be extra mindful of the information you're sharing on it.
- Use two-factor authentication. Using two-factor authentication to protect your online accounts is one of the most effective steps you can take to protect client information.
- Don't use live mic technology. Avoid putting client information at risk by removing voice search or virtual assistant technologies in offices where confidential meetings take place.

In short, you want to do everything you can to prevent unauthorized access to client information.

Learn more about attorney-client confidentiality in our on-demand webinar: Client confidentiality in the digital age.

Evidentiary concerns

When it comes to evidentiary concerns, we're going to go back to law school for some of you. And that is definitely being mindful of attorney-client confidentiality and the work-product doctrine.

But, inadvertent disclosure by a client is not necessarily a waiver.

If the disclosure is inadvertent—as in, not intentional—privilege can survive. If the holder of the privilege or protection took reasonable steps to prevent it—for example, if they weren't necessarily blurting it out at a public restaurant, and they had a reasonable expectation of privacy, and they took reasonable steps to rectify the error—privilege could survive an unfortunate utterance.

That makes attorney client confidentiality different from privacy, in that it is repairable, in many instances, but is not inexhaustible.

Product doctrine

You're probably familiar with the work-product doctrine which refers to the fact that documents prepared in anticipation of litigation are not discoverable.

Now this, again, is an evidentiary rule. It means that opposing counsel cannot request—and you can refuse to provide—certain types of documents in the course of litigation.

However, there are always exceptions to these types of things. One can discover these materials if there is a substantial need for the materials to prepare their case. And so, you, while wanting to keep information private on behalf of your client, may not necessarily be able to do so within the rules of civil procedure and the case law that surrounds privilege.

Ethics concerns

Everybody should be familiar with theRules of Professional Conduct. You probably have used a similar version of these in any jurisdiction that's out there. So we know that they've been mostly adopted by all 50 states (California is the exception). And, analogous versions of these exist in every jurisdiction where Clio customers practice.

Now, there are many different types of grievances on what informed consent is. There are some exceptions built in automatically, whether it's to prevent harm (or a crime), to mitigate harm or an injury, to establish a claim for the lawyer if you're getting sued for malpractice, or to comply with another court order. While it seems like an inexhaustible rule, there are quite a few exceptions.

Statutory concerns

Privacy is mostly created by statute. There are some judicially created types of privacy, but what we're going to focus on are the regulatory concerns with keeping information private. Most of these focus on what's called "personally identifiable information," or PII. PII is any information that can distinguish or trace an individual's identity, or that is linked or linkable to an individual.

Pay attention to business privacy laws

When you start thinking about these rules, you need to start thinking broadly. It's not just your location you need to worry about, but the locations of all of your PII and all of your clients and contacts. Currently we have47 different states that have notification breach laws. And, the U.S. Chamber of Commerce is now calling for a national standard for notification breach laws.

Essentially, they're asking that businesses that leak PII or have a breach, must notify all affected parties. They may have a reporting duty to regulators—and that's normally not your bar association or your court, but actually, the Secretary of State or another government body.

Technology and attorney-client confidentiality

There are three types of safeguards that you need to think about as reasonable for maintaining privacy within your law firm:

- Administrative
- Physical
- Technical

Administrative safeguards mean you have control over who has access to your records and can report quickly and easily on that. This is integral when it comes to attorney-client confidentiality.

And, while physical safeguards are the type of security that you probably already have—you lock your office, you have a password on your phone (you do have a password on your phone, right?) you don't leave things in the back of taxis (because you don't take things in the back of taxis)—it's the technological security issues that are tripping up a lot of businesses and can trip up a lot of lawyers.

Four Tips for keeping your law firm secure

1. Use confirmed technology

First, use confirmed technology. Don't rely on the vendor's word that they're secure, but instead, make sure that they're providing third-party certification, and that all their information is up-to-date. An example of this is onClio's security page, where you can take a look at daily audits. You can take a look at the independent embedding of our privacy

policy, and you can even take a look at our encryption certificates that verify that we're using up-to-date encryption certificates. Looking at something like this is a great way to make sure that you are using encryption and encrypted connections as a part of your service.

2. Set permissions, use two-factor authentication

An important aspect of attorney-client confidentiality is having tools which can provide permissions. You should be able to limit access only to those people who need it.

Ensure that it is difficult to unlock. Many people fail to do this when it comes to securing confidentiality and privacy with their own tools—they don't use security measures like two-factor authentication or separate passwords for each tool.

3. Monitor logins

Making it hard to unlock your information prevents a lot of people from being able to access it. But attorney client confidentiality doesn't end there—you still have to double-check. Ensure you're using tools that give you the ability to see who's logging in, where they're logging in from, and the last accessed date. You can use this information in a tool like Clio to revoke access.

For example, if you see a strange logins from multiple unknown locations, you can force a reset on that password. You can also prevent them from logging in in the future, and then go back and see what, if anything, has been changed using Clio's Firm Feed tool.

4. Use secure communication channels

A law firm client portal — where you share information over encrypted connections, including documents—is key for creating privacy and confidentiality. It's also a good idea to use tools like Signal, an encryption app that's very similar to WhatsApp, but that has much better security and a much better track record of fighting subpoenas for that information. These are all tools that you should be building into or adjusting as part of your practice.

Final notes on attorney-client confidentiality

Attorney-client confidentiality can be thorny. Depending on your practice area and firm size, your process and approach to protecting client information may vary. The one constant is every legal professional should prioritize attorney-client confidentiality to protect both their clients and their firms.

About Clio

Clio is the global leader in legal AI, powering legal work across the profession, from law firms of every size to corporate legal teams, government agencies, and courts. Its Intelligent Legal Work Platform unites the business and practice of law, connecting the people, information, and processes behind legal work. Clio's AI brings the context together with legal sources drawn from Clio Library, a growing collection of more than one billion legal documents. Over 400,000 legal professionals in more than 130 countries rely on Clio to run their legal world. Learn more at www.clio.com.