

Sharing Secure Legal Documents: Client Portals vs. Email Attachments

After years of practicing law, you might not find clients' sensitive data very exciting from a personal perspective. Still, from cyber attackers targeting law firms [alongside U.S.-based defense contractors](#) to run-of-the-mill identity thieves ramping up their efforts, hackers find all types of confidential law firm data just *fascinating*. It's got everything hackers look for, such as:

- Details about mergers and acquisitions
- Attorney-client privileged information about cases
- Litigation strategies
- Social security numbers
- Driver's license numbers
- Credit card numbers
- Bank account information
- Street addresses
- Personal telephone numbers
- And more

The obligation for attorneys to protect clients' confidential information is nothing new. Still, with over of [law firms experiencing a data breach](#) at some point, the American Bar Association (ABA) is sounding alarms about the importance of data security now more than ever.

Failing to invest in reasonable data security measures to protect this veritable gold mine of data leads to major consequences. Even if an attorney's office compromises a client's personally identifiable information (PII) by accident rather than negligence, reprimands and revoked licenses are an imminent threat.

ABA [Rule 1.6: Confidentiality of Information](#) directs attorneys to take every reasonable step to protect attorney-client privilege, and [Formal Opinion 477](#) encourages the use of encryption to do so.

Depending on your preferences for [secure file sharing](#), there is some flexibility when it comes to upholding your legal and ethical data security obligations. Communicating with clients via secure client portals and sending encrypted email attachments via a secure file-sharing platform are both acceptable options.

Like in all matters, though, each approach has pros and cons. To help you decide on a legal file-sharing strategy, we'll outline the basics of both secure client portals and encrypted email attachments below.

Sharing legal documents within secure client portals

When secure client portals were first invented, they were clunky and difficult for an average person to navigate without training. The only clients that truly embraced the technology were those with a strong technological background. But in the late 2010s, data security threats drove attorneys to the security offered by client portals in an effort to protect client confidentiality.

And to their credit, client portals have come a long way in recent years. Increasingly intuitive and multifunctional, they offer a better user experience than in their early days.

Pros of secure client portals for legal file sharing (and beyond)

The number one use of secure client portals is legal file-sharing, but they're also a digital "one-stop shop" for other critical interactions between attorneys and clients. This comprehensive method of communication does much more than protect client confidentiality.

Clients can use a [secure client portal](#) to upload photographic or video evidence, make appointments to meet with an attorney, send secure messages, and view attorneys' work in progress on their legal matters. Law firms might also let clients view trust account balances and pay legal bills within the secure client portal.

This consolidation saves attorneys time digging through inboxes and email threads for pictures, phone numbers, and questions.

But what feels advantageous to attorneys isn't always embraced by clients.

Cons of secure client portals for law firm file-sharing

Client perception of legal file sharing via [secure client portals](#) is that it's generally safe. But that positive perception is tempered by some criticism—namely, those client portals aren't as easy or familiar as email. As a result, some individuals are willing to sacrifice confidentiality for convenience.

To access files, the client must open an emailed invitation to join the client portal, enter the provided credentials, and create an account with a unique password. From there, it's time to learn to navigate the interface. When difficulties arise, attorneys may need to act as tech support to help clients access their documents.

These “extra steps” may potentially slow down legal workflows.

Sending encrypted email attachments via secure file-sharing platforms

As a familiar tool that most people already use regularly, email is primed for legal file sharing. The key is that extra measures *must* be taken to do so without jeopardizing data security.

As a result, legal file sharing over email has been a source of debate for decades.

Is it safe?

Is it ethical?

Should attorneys compromise on data security by using email attachments for law firm file sharing per a client's request?

Pros of using email for legal file sharing

Fortunately, [secure file sharing platforms](#) have emerged to make truly secure file sharing over email possible using encrypted attachments and

links. The ability to add an expiration date to encrypted legal file sharing links adds an extra layer of protection against cyber attacks.

These law firm file sharing platforms offer versatility and convenience. Clients and colleagues don't need to log into a separate site or software to review legal documents. The interface is intuitive, too. Clients rejoice that they won't have to spend their mental energy creating another username and password.

Law firm file sharing via encrypted email attachments can also speed up legal workflows because access to important files is nearly instant—without compromising client confidentiality or data security.

Cons of Legal File Sharing Over Email

Opening the door to law firm file sharing via email is confusing for some clients. Many people don't understand the nuances of data security when communicating via email. Encryption can be a foreign concept for people who don't manage sensitive data every day for work.

Under the misconception that unencrypted standard emails are a secure file sharing method, clients may respond to attorneys' secure communications with personal details or sensitive documents attached as standard, unencrypted attachments.

Another downside is that some clients infrequently check their email. They may struggle to find the proverbial needle in a haystack within pages of spam and marketing newsletters. When they *finally* find the correct email, discovering that the secure file sharing link has expired can be frustrating for both attorney and client.

Even clients that do check their email regularly might not recognize the role secure file sharing platforms play in sharing legal files via email. As a result, they could mistakenly perceive highly encrypted links to important documents as unsecured.

Secure client portal vs. encrypted email attachments: which is better for legal file sharing?

The question stands, though. Are secure client portals or encrypted email attachments preferable for sending legal documents and sensitive personally identifying information?

As long as you take every precaution to protect client confidentiality and prioritize [data security in your law firm](#) file sharing practices, there's no "right" answer.

Both methods offer significant protection against cyber threats and identity thieves—and proponents and critics abound on either side. Ultimately, the decision to use a secure client portal or encrypted email attachments for secure file sharing comes down to which option best serves the needs of your clients and your staff.

TimeSolv Supports Convenient Law Firm File Sharing

For many, adopting a legal file-sharing strategy that combines a secure client portal and encrypted email links is an effective way to meet clients and colleagues where they're at. This approach accommodates individual preferences for legal file sharing, which increases the likelihood that the intended recipients of sensitive documents will receive them promptly while upholding strong boundaries about data security.

For your convenience, TimeSolv offers multiple secure file sharing options, including seamless integration with [LexShare](#).

Whether you prefer to use a [secure client portal](#), safely [send legal documents via email](#), or some combination of both, with TimeSolv, protecting client confidentiality is simple and convenient.

See secure file sharing with TimeSolv in action first-hand! Contact us to [schedule a demo](#) or begin your [free trial](#).