Wolters Kluwer

When you have to be right

Secure File Sharing

5 Ways Law Firms Can Mitigate File Sharing Risks

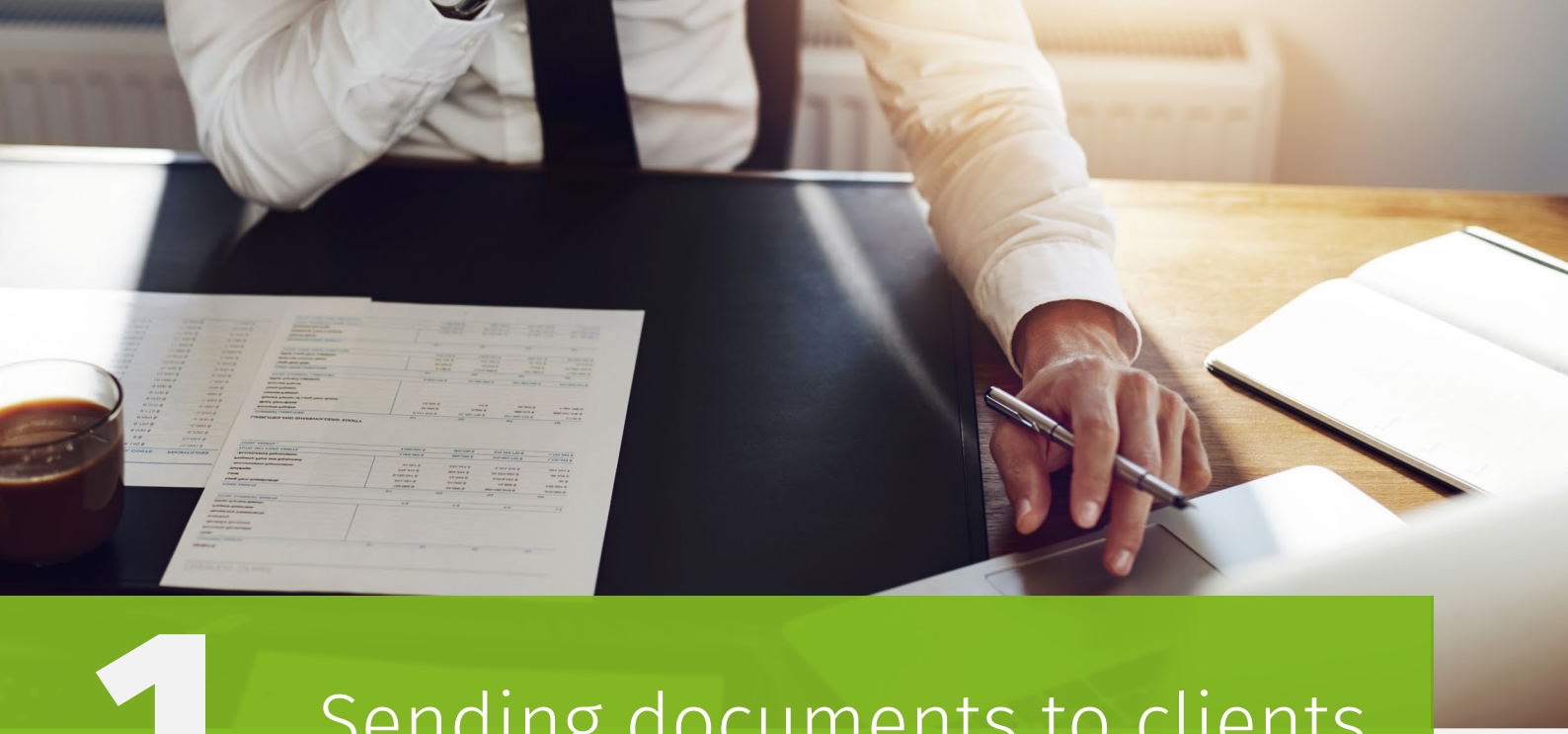
5 Ways Law Firms Can Mitigate File Sharing Risks

File sharing isn't a new concept. The need to send documents back and forth is as old as time itself.

In the digital age, lawyers are exchanging documents with colleagues and clients on a daily basis. However, as email and cloud-based file sharing services become the norm, we need to examine the inherent security risks associated with these digital methods and their impact on how we conduct business.

Furthermore, law firms are subject to rigorous confidentiality obligations, professional secrecy and third-party data protection, which require additional effort on the part of employees to prevent non-compliance and avoid data loss.

Secure file sharing starts with educating everyone about the risks and implementing standards to govern file sharing practices. Here are 5 ways your law firm can mitigate file sharing risks with appropriate security measures.



1 Sending documents to clients

THE SCENARIO

You need to send a document to a client for them to review and sign. While you used to have the client come into your office to sign it or send it via courier, technology let's you speed up this process by sending the document via email. The client can print the document and review it before returning the signed hard copy.

Mitigate the risk: Use a secure cloud-based portal that is protected with encryption and passwords.

Printing hard copies of confidential legal documents can expose you to a variety of risks including tampering, forgery, loss or theft which can result in data breaches that can have disastrous consequences for your firm and clients. Using a secure service with encryption and passwords ensures that only registered users - like clients or other third parties - are able to access the information you are sharing.

When considering a cloud-based service it's important to note that many consumer-grade services can leave you open to data leaks and other security threats. Law firms need a business-grade service that allows users to control who can access documents, when they can access it (ie. expiring access) and alerts when users upload or download a document. Also, cloud-based services that are built for law firms have the added feature to provide audit trails in the event you need to generate compliance statements.

2 Collaborating on documents with colleagues

THE SCENARIO

From time to time, you need some advice on a document from colleagues in your firm. You've been drafting the document on your computer so you quickly attach it to an email asking for their feedback. At the same time, you realize that you want give some other colleagues access to the document so you drag it over to a shared drive folder on your office network.

Mitigate the risk: Invite colleagues to review documents directly from the cloud-based service.

While we may hate to admit it, security breaches and data leaks can start internally, so the best way to mitigate risk is by limiting file access. You can never have 100% control over who will access your document if you send it via email or post it to a shared folder that others may have access to.

With a cloud-based file sharing service that facilitates document collaboration, you invite only those authorized users who you want to access, comment or modify your document. Also, with a cloud-based service that is built for law firms, you can get an audit trail on who has viewed or downloaded your document and when they have accessed it. The result is a paperless workflow for contracts and other legal documents that protects your firm from data leaks and other security threats.

Finally, when considering a cloud-based service, it may be tempting to pick a system that simply let's you share files and collaborate, but you should also consider an integrated solution that offers additional capabilities, like case management or invoicing.

3 Storing documents

THE SCENARIO

As a lawyer you often have to handle documents that contain sensitive, confidential information regarding your clients. However, after a certain amount of time passes, you need to decide how to store or destroy documents that you no longer need. In the past you would shred document in a secure manner, but now with electronic files you're not sure what to do. Until you find a better system, you've archived these documents in an external hard drive.

Mitigate the risk: Store files in a cloud-based repository with archiving.

Lawyers need to implement document management policies that cover the collection, transmission, maintenance, and storage of client information, including documents stored in hard copy, electronically, or remotely, or covered by a confidentiality agreement or court order, for each client.

When information is scattered across many different documents, it can be difficult to get an overview of everything. A cloud-based repository can help you store all of these documents and then set up document retention procedures as required.

Furthermore, cloud storage services built for businesses, and specifically for law firms, are continuously backed up to protect you against data loss and offer unlimited storage to meet your needs. Consumer-grade services like OneDrive, Dropbox and iCloud can have the disadvantage of lower storage capacities and lower security depending on the ability to encrypt data or how account security settings are configured.

When you decide to take action to safe-guard your data storage, implementing a cloud solution makes it easy. Choose a business-focused cloud service that offers speedy setup and ongoing agility, as well as unlimited storage. management or invoicing.

4 Acknowledging the receipt of documents

THE SCENARIO

It's important to know when your client receives documents, especially when time is of the essence like during contract negotiations. When you courier or email documents to your client, you always request a delivery receipt or read receipt, so that you know they have the documents in hand.

Mitigate the risk: Receive alerts and maintain an audit trail on documents your client accesses on an online portal.

As we've already established, sending hard copies or emailing documents with confidential information can expose you to risks since you can't always have 100% control over who sees them.

When you use an online portal to share documents not only do you control who has access to it thanks to user authentication, but you can also receive alerts that notify you as soon as a document has been accessed. Not only does this give you an immediate status on the delivery of your document, but if you're using a system built for lawyers, it should provide audit trails in the event you need to generate compliance statements.

5 Remote access to documents

THE SCENARIO

Meetings away from your office are a daily occurrence and it's vital that you have important documents with you. You used to bring hard copies of pertinent contracts and agreements with you, but now that you can easily travel with your laptop, you save files on your desktop so you can access them quickly during meetings. In some circumstances, you save files to a USB drive so you can pull them up on your client's computer.

Mitigate the risk: Use a cloud-based document management system where you can always access documents anywhere from any device.

While encryption programs can help protect your information on external drives, if you're opening documents to another person's computer or if you lose the information (and haven't saved it anywhere else), you could be exposing yourself to a variety of security risks.

The best way to access documents when you're not in the office is to use a secure cloud-based system. However, if the system you have adopted is over complicated with rules and cannot be accessed outside the office or on mobile, it will be hard to get everyone using the same level of diligence. When systems are overly complicated, users are deterred from logging in and find alternative, unsafe methods to share and access files. When choosing a system, ensure it's easy for everyone to use, anywhere they are. While it's important to mitigate risks and meet necessary security requirements, if the system is not easy to use, it will be hard to get people to adopt it.

Conclusion

Law firms not only need a secure method for sharing information, but a system for monitoring access to the documents, including when and with whom information has been shared. Diligent monitoring is the first step to preventing data mismanagement.

To a lawyer, client data security is paramount. Don't risk your data security with any file sharing platform. With Kleos' secure file-sharing function, share confidential files in a safe channel. Discover Kleos Connect, the secure and innovative document sharing functionality of Kleos.

LEARN MORE ▸

If you want to find out more about Wolters Kluwer cloud-based Legal Solutions, visit our website: kleos.wolterskluwer.com