White Paper

6 Best Practices for Law Firms to Protect Sensitive Data in the Cloud

A primer on attorney-client file sharing

CipherCloud®
Trust in the Cloud™

333 W. San Carlos Street
San Jose, CA 95110

Table of Contents

INTRODUCTION

File sharing is a common way for attorneys and clients to share confidential and privileged information. Cloud-based tools make attorney-client communication easy and quick. Part of the appeal of cloud applications is that users can easily set up accounts and use services without involving their IT departments, a trend otherwise known as Shadow IT.

The convenience of cloud applications comes with risks, such as data leaks, breaches of confidential information, and non-compliance with data privacy regulations.

In a 2014 survey of US law practices by LexisNexis®, a majority of respondents (including practicing attorneys and other legal professionals) said that they're concerned about possible data breaches and that they use consumer file sharing services. Awareness of risks while taking risks is a clear sign that attorneys need help to securely use cloud-based file sharing. Indeed, providing this help is an important part of law practice management.

Following are key best practices for law firms of all sizes that want to to enable cloud-based file sharing while protecting sensitive data.

BEST PRACTICE #1:
KNOW YOUR CLOUDS

When it comes to cloud security, what you don't know can hurt you. Before you can secure data shared in the cloud, first know your clouds.

Start by identifying the cloud-based file sharing and collaboration tools that are important to your firm's legal professionals and clients.

Then, identify the types of sensitive information shared on each platform and note where that data is stored.

Finally, list the data risks inherent in each cloud-based platform.

> "When it comes to cloud security, what you don't know can hurt you."

BEST PRACTICE #2:
CONSOLIDATE YOUR CLOUDS

It's a good idea to standardize your firm's cloud-based file sharing services, partly because it reduces cloud monitoring overhead. At the same time, be sure to take the time to understand why your legal professionals have adopted a particular file sharing service. Does it have unique product features that are important to users? Is it more usable than other services? Is it more commonly used on the client side?

Once you have a complete list of the clouds involved, sanctioned or unsanctioned, narrow the list by weighing the risks of each platform against its popularity among attorneys and clients. This way, you'll have fewer clouds to monitor, but you'll still enable attorneys to use the services that they and their clients prefer.Keep in mind, however, that you'll never consolidate to the point of having only one file sharing application. You need a multi-cloud strategy.

BEST PRACTICE #3:
KNOW (AND MONITOR) YOUR USERS

All user access, from senior partners and legal secretaries to clients and other outside third-parties, should be managed centrally.

1. Give each user in the firm only as much privilege and access as necessary to perform his or her job easily. Be cautious about extending admin privileges.
2. As many attorneys rely on legal secretaries to perform some communications on their behalf, ensure that legal secretaries (and all other users) have their own credentials.
3. In addition, you should identify all clients and other third parties such as suppliers or consultants and ensure their access levels on each platform don't exceed their collaboration needs.
4. For all users, identify their locations and the devices they use to access client data.
5. Knowing is more than identifying. It also means knowing what users are doing. Monitoring activity continuously is important for providing a complete log of a user's activity should an audit be necessary. It also enables you to act quickly should you identify anomalous activities such as unusually large downloads of privileged data or repeated login attempts from unfamiliar IP addresses.

BEST PRACTICE #4:
SET POLICIES AND DOCUMENT THEM

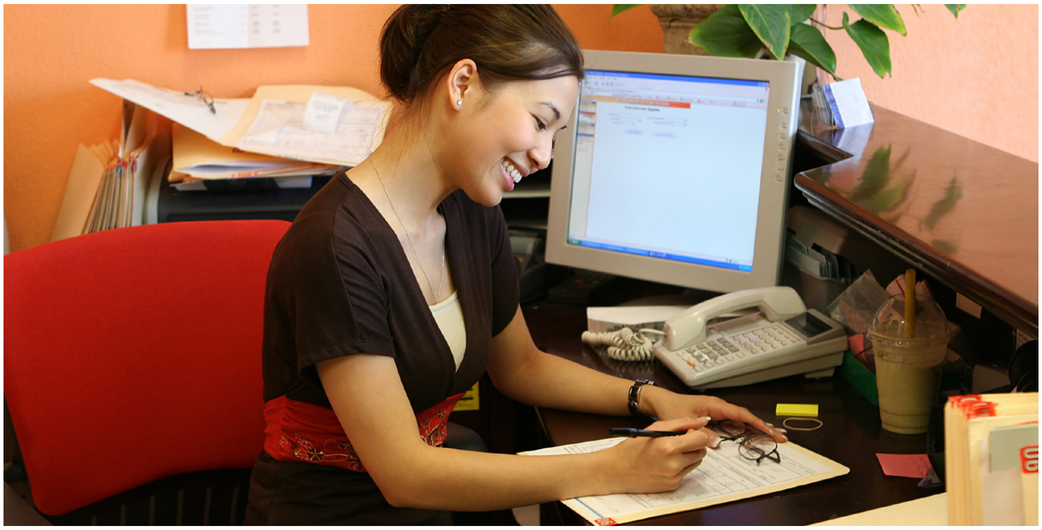
When setting policies, define the services that are sanctioned and how user accounts will be handled.

- When an employee leaves the firm, how will their account be handled?
- How are user names defined? Can employees change their user names?
- Will you disable persistent login? We recommend that you do.
- What is the maximum number of failed login attempts before an account is disabled?
- Will you require login verification? We recommend that you do.
- In what instances, and why, will you have admins, co-admins, and group admins?

BEST PRACTICE #5: IMPLEMENT A CLOUD ACCESS SECURITY BROKER SOLUTION

Even when cloud-based file sharing activity is appropriate, your firm has no visibility into who has access to a file once it leaves your network. After all, no law firm is an island entire of itself. Fortunately, implementing one of the best Cloud Access Security Broker (CASB) solutions gives you robust data security with policy-based encryption, so unauthorized users can't access sensitive files even after the data has left your network.

Moreover, implementing a CASB solution will enable you to easily support multiple file sharing and collaboration tools with consistent policies for data loss prevention, collaboration controls, and remediation across your set of clouds. Once you've defined your desired level of control, you'll be able to monitor user activity and file use trends, detect anomalous behavior, and take action immediately.



BEST PRACTICE #6: EDUCATE AND INFORM EVERYONE

Once you have defined clear policies, processes and procedures, and implemented a CASB solution such as CipherCloud, it's time to educate and inform employees. Remember, data security concerns everyone, not just current users. Involve everyone, including attorneys, paralegals, legal secretaries, and anyone else who may need access to cloud-based file sharing applications.

SUMMARY

By knowing your clouds and your users, documenting policies, implementing a CASB solution for a multi-cloud strategy, and educating your employees, your law firm can stay abreast of emerging best practices to protect sensitive information. Implementing these measures also means you'll be able to demonstrate both compliance with data privacy laws and reasonable care to protect sensitive information, thereby protecting your firm from expensive malpractice claims and government fines. Best of all, you'll enable efficient file sharing and collaboration across your firm's favorite cloud-based applications.

Get Protection Now!

To see how a CASB solution like CipherCloud can help your law firm protect sensitive data, register for a Free Trial of CipherCloud.

LexisNexus, "File-Sharing in the Legal Industry: Survey uncovers disconnect between security fears and the everyday practices that can leave firms open to breaches," in Business of Law Insights Report. New York: New York, 2014.

CipherCloud™
Trust in the Cloud

CipherCloud, a pioneer in delivering cloud information protection, has just announced its new GDPR-ready solution. With CipherCloud, you can deliver better business results by overcoming the risks of data privacy, residency, security, and regulatory compliance. Our unique and innovative technology protects the entire lifecycle of your data, including discovery, encryption, tokenization, data loss prevention, malware detection, and ongoing monitoring and anomaly detection of your users' cloud activity.

Headquarters:
CipherCloud
333 West San Carlos Street
San Jose, CA 95110
www.ciphercloud.com

linkedin.com/company/ciphercloud
@ciphercloud
sales@ciphercloud.com
1-855-5CIPHER (1-855-524-7437)