LEGAL workspace
Your Law Office in the Cloud

Should responsible law firms use CLOUD STORAGE?

Learn more about protecting privileged information in the cloud.

LEGAL workspace
Your Law Office in the Cloud

Protecting Data in the Cloud

Protecting privilege is one reason law firms have been hesitant to adopt using the cloud for document storage and sharing. Fears of hacking or inadvertently providing access to privileged documents have kept many firms from embracing technology that could save them time and money.

Most tech-savvy law firms have taken precautions and put protocols in place to secure client documents and communications as they've upgraded to cloud sharing. However, some firms have been lax in their safeguarding procedures — which means their clients were left unprotected.

Unprotected file-sharing

You've likely heard of file-sharing options such as Box, Google Docs, OneDrive or Dropbox. Free cloud storage options like these allow users to access documents from any device and to share files by creating custom URLs. They're convenient, and — when used properly — can be a secure way to share information.

A problem arises when users take shortcuts or don't take advantage of all of the security features available in cloud storage and sharing systems. That's what happened with *Harleysville Insurance Co. v. Holding Funeral Home*. Harleysville's counsel shared privileged information via Box, using its feature that creates direct links — and they didn't password-protect the links. That meant that anyone who had access to the link could see the files. As a result, the defendant's counsel was able to access this information.

A Virginia magistrate recently ruled that the plaintiff's law firm's actions "were the cyber-world equivalent of leaving its claims files on a bench in the public square and telling its counsel where they could find it." In other words, its failure to password-protect and otherwise secure those files waived privilege.

Use the cloud safely

This ruling doesn't mean that law firms should discontinue cloud usage. Rather, it emphasizes the importance of putting security measures in place to block access and uphold attorney-client privilege.

Here are some ways to keep your data in the cloud secure:

1. Require log-ins (on both sides of the fence—attorneys and clients) to gain access to shared information.

2. Keep access contained. Only permit a select few team leads to share information with additional parties.

3. Some programs have a "notify when accessed" feature. Using this feature tells the content owners how and when the information has been accessed — so if there is unauthorized access, you'll know about it right away.

4. Put an expiration date on the shared information. It's better to re-share the information than to let it dwell on the internet in perpetuity.

Legal Workspace recommends that law firms use document management and file-sharing programs created specifically for law firms such as iManage, NetDocs, Citrix Sharefile and Egnyte. That way, you know the technology was created with attorney-client privilege in mind.

Legal Workspace provides a base package with its cloud environment service and encourages clients to customize their environments to incorporate legal applications to formalize their processes and take extra steps toward protecting attorney-client privilege.

The cloud can be a safe place. Document sharing over the cloud can be secure. Law firms simply need to understand how breaches can occur and take precautions to protect all parties using the cloud.

If you have any questions about safe cloud sharing, feel free to reach out to our legal app experts.

Legal Workspace is a pioneer in cloud-based work environments and data storage designed specifically for law firms. Learn more at legal-workspace.com.