The Ethical Considerations of Moving Your Law Firm's Data to the Cloud

Cloud computing is not only the wave of the future but also the wave of the present as more and more businesses are using remote cloud servers offered by Google, Dropbox, and host of other data providers to reduce their internal storage costs while providing reliable backups of company documents, easily accessible by employees from both the office and at home.

But attorneys of course must follow ethical guidelines in how they conduct business, and sharing client information with third-parties brings up issues related to their duty of confidentiality and obligation to protect their clients from harm. Ethics guidelines will vary from state to state based on state bar association guidance (many useful links to state bar opinions on this issue can be found here), but there are some general ethical considerations all attorneys should keep in mind when utilizing cloud storage.

Exercise Reasonable Caution Based on Foreseeable Risks

In the same way negligence law uses the reasonable person standard to determine whether a defendant is liable, many state bar associations recognize that technology changes far quicker than any set of rules can keep up with, and so they often employ a similarly flexible standard in determining whether an attorney has violated his or her duties of confidentiality and competence when using cloud computing. Your state bar association does not expect you to become a computer privacy expert, but it does expect you to take some reasonable steps to understand the foreseeable risks of cloud computing and take action to mitigate those

risks. As part of this reasonable caution approach, proportionate care should be taken to protect data based on the sensitivity posed by that data.

Be Wary of Using Unsecured Public Wireless

One clear way in which you will want to exercise caution is to avoid exposing sensitive information through unsecured public wireless networks. It is great that Starbucks offers free wi-fi but you will want to think twice before sending an email with sensitive client information on your coffee break if it means others will gain access to it. Similarly, do your research on your hotel's wi-fi security policy before doing important work over its network.

Use Outside Consultants When Necessary

Again, no one expects you as an attorney to know the details of how your cloud computing works and specifically how data privacy and security is maintained, but it is your responsibility nonetheless to see that that privacy and security is maintained. If you need to work with an outside consultant to make that happen, then state bar associations will no doubt want to see that that occurs.

Obtain Enforceable Obligations to Maintain Security from Vendors

Many law firms outsource much of their backend work involving document processing and storage to outside vendors these days. You should make sure that your contract with those vendors contains appropriate safeguards for your client's data security as well as a right to enforce the contract on behalf of your clients if the vendor fails to live up to protect the data.

Get Started with TimeSolv Today

TimeSolv offers backend automated office solutions that brings big-firm innovation to all types of firms, no matter the size. To start your free trial of TimeSolv today, click here.