LEGAL workspace
Your Law Office in the Cloud

9 DATA SECURITY QUESTIONS

YOU SHOULD ASK YOUR IT PROVIDER

Learn more about today's cloud computing solutions for law firms.

LEGAL workspace
Your Law Office in the Cloud

9 Data Security Questions You Should Ask Your IT Provider

Wondering how secure your data is? Ask your cloud, SaaS, or existing IT provider these nine questions to make sure it's protected. Their answers could mean peace of mind—or they could mean that your future will hold a data breach, data loss, or a cumbersome recovery process after a disaster.

1. Do you have an intrusion prevention detection system?

An intrusion prevention detection system (IDPS) senses strange traffic on your server. Hackers continually scan IP addresses, searching for vulnerabilities. An IDPS recognizes when they're attempting to break in and cuts off their access.

Occasionally, a user can inadvertently mimic the signs that an intruder is attempting to break in. For example, someone might enter the wrong passcode into a smartphone, and cause a glitch to occur where the phone tries repeatedly to log into the system. Does your provider have round-the-clock security staff to restore access in case something like that happens?

2. Do you support two-factor authentication?

Two-factor authentication requires two components for an attorney to log in. This type of authentication makes it impossible for a person or an automated system to log in to a computer by remote and start guessing passwords.

Here's one example of two-factor authentication: When a user logs in to his or her system, a mobile application confirms that the user is trying to log in. The user cannot log in to the system until the user has confirmed his/her identity on the mobile device.

3. What government/industry security standards has your environment been tested for?

Many providers use generic terms like "bank grade" or "enterprise" security, but those descriptors don't necessarily mean that they conform to strict security standards required for Payment Card Industry (PCI) or Health Insurance Portability and Accountability Act (HIPAA) compliance.

LEGAL workspace
Your Law Office in the Cloud

Any law firm with clients who store, transmit or access protected health information must be HIPAA-compliant. Depending on the sensitivity level of your data, your cloud, SaaS, or IT provider should maintain an environment that meets the security standards you need. It's also necessary for any business that accepts credit card payments to be PCI-compliant.

4. What type of firewall are you using?

The answer you should hear from your provider is: an enterprise-grade firewall that is routinely patched. An even better answer would be that the provider has more than one of those firewalls in place. That way, if one firewall fails, there's another present to act as back-up.

5. Are the employees who have access to my information data-certified? Do they have certification on security procedures?

This is an important question to have answered because who can access your data (and their level of experience and expertise) could mean the difference between mishandled information and security. Administrators that have access to clients' data should have information security certifications, specialized training, and execute non-disclosure agreements.

6. Do any third-party providers have access to your hosted environment?

Let's say that there's a problem with an application hosted on your environment. What protocol does your cloud, SaaS, or IT provider follow? Does it allow the application vendor onto the virtual server? If so, that gives a third party access to all of your data, which puts it at risk and violates the HIPAA standard.

7. Does the cloud, SaaS, or IT provider support encryption of data on the server, including email?

Email is an often overlooked factor in data security. For it to be completely secure, it should be encrypted—even when in rest or in transit. This is the most common security vulnerability because constructing the appropriate security measures is difficult for a typical IT department to do; it's a complex process that requires a high level of expertise.

8. Do you routinely perform internal and external security scans to seek vulnerabilities?

A provider might believe that they've set up a secure environment—but technology is constantly changing, which means that the ways in which intruders attack are constantly changing.

To make certain that your data is protected, your provider should be performing security scans regularly. These scans are required for both PCI and HIPAA compliance; to be HIPAA-compliant, both an internal and external security scan needs to be performed at least once a year.

9. Does your provider have a secondary site for data storage?

What happens if all of the redundancy fails and a major disaster strikes? If something, such as a theft or fire were to happen at your location, are your disc back-ups replicated offsite? Many organizations omit that step. And, even if you do store back-ups at a secondary location, is that location secure? Do only your provider's employees have access to the data at that location—or can a third party access it as well?

If your data is replicated and secure, how long will it take you to get back up and running? It could be hours. It could be days.

Constant protection

Redundancy is built into every security measure at Legal Workspace. That means clients' data is constantly being monitored and protected.

Legal Workspace's HIPAA Compliant Edition (HCE) achieves the highest level of data security because it is both PCI- and HIPAA-compliant. Employees are all HIPAA-certified and have additional information security certifications. They're the only people that have access to your data: third party vendors aren't permitted to access Legal Workspace's environment.

There's no need for attorneys to be concerned about email vulnerability; Legal Workspace encrypts email in transit and in your inbox. And, clients' data gets backed up to a second data center, which means that you could be back up and running within minutes in the aftermath of a disaster.

It's very difficult for a small—or even a medium-sized—law firm to build a solution that answers all of these questions appropriately. . . working with an expert in data security and cloud services for law firms, like Legal Workspace, will give your law firm the highest level of security at a fraction of the cost to do it on-site. Keep your data secure and protected by making sure the best safeguards are in place.

Legal Workspace is a pioneer in cloud-based work environments and data storage designed specifically for law firms. Learn more or arrange a free demo at legal-workspace.com. Click here to watch our video.