Is the Cloud Safe for Law Firms? Key Ethical and Practical Considerations

Many law firms already use cloud tools. They use them for email, file sharing, and practice software. The real question isn't whether your firm should move to the cloud—that's where all legal software is eventually headed. The question is which cloud tools are safe, and under what controls.

Lawyers still have duties. Confidentiality matters. Supervision matters. Competence matters.

This article answers the most common questions firms ask before moving client data to cloud tools. You'll also get a practical checklist and best practices to vet vendors, set the right controls, and protect client information throughout the transition.

How Do Law Firms Use the Cloud?

Law firms use the cloud to store and access data without keeping everything on an office server. Staff can work from the office, home, court, or while traveling. Files and updates stay in sync.

A recent American Bar Association legal technology survey found that around three-quarters (75%) of lawyers are using cloud-based tools for work today.

Common cloud uses within a law firm include:

- Email, calendars, and project/task management
- Document management, storage, and sharing
- Practice management, time tracking, and billing software

- Messaging, client portals, and client collaboration tools
- Client Relationship Management (CRM) software
- Legal payment processing
- Backups and disaster recovery

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.

Many firms are already using "cloud-only" tools for their enhanced security features and flexibility for remote or out-of-office work. Others still use a mix of cloud and on-premise systems. Either way, client data often ends up in cloud services through daily work.

Can the Cloud Be Trusted by Law Firms?

The cloud can be safe for law firms when you choose the right vendor, configure it correctly, and train your people.

Using the cloud is not automatically a risk. Using it without clear controls and risk management is. Most ethics guidance uses a "reasonable efforts/reasonable care" approach. That means you match safeguards to the sensitivity of the data and the foreseeable risks.

In fact, security and confidentiality concerns surrounding cloud computing and technological advancements prompted the ABA to amend Model Rule 1.6 to make these responsibilities an ethical obligation between lawyers and clients.

The latest guidance states that lawyers must *"make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client."*

That duty applies regardless of whether data is stored on a local server or in the cloud. Using cloud-based software does not reduce that responsibility. It raises the importance of understanding how client data is protected, who

can access it, and what safeguards are in place to prevent mistakes or breaches.

To meet that standard, firms need to look beyond surface-level security claims.

Let's review four practical areas that matter most when evaluating cloud-based software. Each section focuses on what firms should understand, what questions to ask, and how to apply reasonable safeguards in real-world use.

Your Duty of Confidentiality and Control in the Cloud

The duty of confidentiality still applies regardless of where information lives or what format it is in. Cloud tools can be safe, but only when the firm stays intentional about protecting access and preventing disclosure.

The "reasonable efforts" ethics standard is important. In plain terms, that means you should understand the potential risks of storing data in the cloud and take steps that match the sensitivity of the information.

Highly sensitive client data deserves stronger safeguards. Less sensitive data may require fewer controls.

A big part of that standard comes down to control. When you store client data in a cloud platform, you are still responsible for how that data is accessed, shared, and safeguarded. You do not "hand off" responsibility to the vendor.

- You control **who can access** client data.
- You control **how access is granted** and removed.
- You control **how data is shared** outside the firm.

- You control **how long data is retained** and how it is destroyed.

You have a plan if the vendor is served with legal process (including notice when allowed).

Quick Cloud Confidentiality Checklist

Before you review features or vendor claims, it helps to ground cloud decisions in a short, practical checklist.

These are baseline steps most firms can take to demonstrate reasonable care and maintain control over client information when using cloud-based tools.

- Use Multi-Factor Authentication (MFA) for every user.
- Use role-based access wherever possible.
- Turn on audit logs to maintain complete records.
- Set sharing permissions to “least access needed.”

Require breach notice terms in your contract.

2. Competence, Supervision, and Vendor Due Diligence

You’re not expected to become a full-time security engineer to use cloud software responsibly. But ethics rules do expect lawyers to understand the benefits and risks of the technology they rely on.

That includes knowing how client data is handled, where it lives, and what happens when something goes wrong.

Ethics guidance also makes it clear that responsibility doesn’t stop at your firm’s walls. When you use third-party vendors to store or process client information, you still have a duty to supervise that work. If a vendor mishandles data, the firm can’t simply point to the contract and walk away.

This is why vendor due diligence matters. Many data breaches are not caused by sophisticated attacks, but because of misconfigurations, weak access controls, or unclear responsibilities between firms and vendors.

In several widely reported incidents across industries, firms were required to notify clients after vendors failed to secure data or delayed breach notification. The lesson is consistent: *you are expected to ask questions before an issue occurs, not after.*

Vendor Due Diligence Checklist: What to Ask

Competence and supervision in the cloud mean asking the right questions up front, documenting the answers, and choosing vendors that can clearly explain how they protect your clients' information.

- What data do you collect and store for our firm?
- How is our data encrypted in transit and at rest?
- Who on your team can access our data, and why?
- What happens if there is a security incident or breach?
- How and when will we be notified after a breach?
- Do you use subcontractors or subprocessors? Which ones?
- How can we export all firm data if we leave the platform?
- What is your uptime, backup, and disaster recovery plan?

Ethics guidance frequently recommends reviewing a vendor's qualifications, reputation, and security practices before engagement. It also points to the importance of written agreements that clearly spell out confidentiality obligations, security expectations, and breach notification requirements.

What control means in practice:

3. Data Jurisdiction, Ownership, and Exit Strategy

Cloud software can feel simple on the surface: log in, upload, and share. But behind the scenes, data can move across locations, vendors, and backup systems. This is where many firms get surprised.

If you don't ask the right questions upfront, you may not learn the limits until you're dealing with a dispute, a client request, or a migration deadline.

Data Jurisdiction: Where Does Your Data Live?

Even if your firm is local, your vendor's infrastructure may not be.

Cloud data may be stored or processed in different states or countries. That matters because location can affect privacy rules, discovery obligations, and the risk of access requests from governments or third parties.

The practical fix is simple. Your vendor should be able to tell you where data is stored, where it is processed, and whether you can choose a data region. If the vendor cannot answer clearly, that's a signal to dig deeper before you sign.

Data Ownership: Who Owns It?

Client data should remain yours, and this should be stated plainly in the contract.

Ownership also includes practical rights, not just legal language. You should understand what the vendor can do with your data, whether data is used to train models, who can access it, and what happens to your information in backups.

A strong agreement also covers return of data, retention periods, and breach notification terms. If those items are vague, your firm's "control" can be weaker than it looks.

Exit Strategy: What Happens When You Leave?

Plan for leaving before you sign a new cloud vendor contract. An exit plan protects you if pricing changes, features change, the vendor is acquired, or your firm outgrows the product. It also reduces risk during transitions, when mistakes and gaps are more likely.

Before you commit, get clear answers to a few practical questions:

- Can you export your data in a usable format that preserves history and context?
- How long will the vendor keep data after termination?
- Will the vendor support migration, and what does that support include?
- What happens to backups after termination?

- How do you confirm data deletion, including backups where possible?

Remember: “We can leave anytime” is only true when export, retention, and deletion terms are spelled out in writing.

4. Risk-Based Security and Ethical Decision Making

Not all client data is equal. Your security decisions should reflect the sensitivity of the data and the likelihood of harm if something goes wrong. The most sensitive data needs the tightest controls.

A risk-based approach will help your firm make practical decisions instead of defaulting to fear or overcorrection. You won’t need the same controls everywhere, but you do need the right controls in the right places.

Use a Simple Risk-Based Process

Start by breaking the problem down into manageable steps.

- Identify the type of data you handle, such as personally identifiable information, medical records, financial details, or privileged communications.
- Identify the most likely threats to that data, based on how your firm actually works.
- Choose safeguards that directly reduce those risks without creating unnecessary friction.
- Train staff on the areas where mistakes are most likely to happen.

Many real-world security issues come from predictable failure points. Addressing those areas often provides the biggest improvement with the least effort.

Common Data Breach Points and Practical Fixes

Most cloud security problems come from everyday behavior, not rare “movie-style” hacks. The good news is that the most common risks are also

the easiest to reduce when you put a few simple cybersecurity controls in place.

- **Phishing attacks:** Reduce risk by training staff to spot suspicious messages and requiring multi-factor authentication for all users.
- **Weak or reused passwords:** Prevent account takeovers by using a password manager, enforcing strong password rules, and pairing passwords with multi-factor authentication.
- **Oversharing links or files:** Avoid accidental exposure by using secure file-sharing software and setting sharing to the most restrictive option by default.
- **Lost or stolen laptops/devices:** Protect client data by using full-disk encryption and enabling remote wipe on firm devices.
- **No clear response plan:** Limit damage by creating a basic incident response checklist, assigning roles in advance, and documenting how and when you will notify clients if required.

Ethical decision making in the cloud means matching safeguards to risk, revisiting those decisions as your firm changes, and focusing on the failures that are most likely to happen in day-to-day work.

Law Firms and the Cloud: Best Practices for Ethical Use

Good cloud security comes from everyday habits that reduce risk and support your ethical duties over time. The following practices address common gaps that show up across law firms of all sizes.

Avoid Unsecured Public Wi-Fi

Public networks make it easier for data to be intercepted or exposed. Even when nothing "goes wrong," unsecured Wi-Fi increases risk in ways that are hard to see in the moment.

- Use a VPN when working outside the office
- Prefer a personal hotspot over public Wi-Fi
- Avoid accessing or sending sensitive client data on unknown networks
- Disable auto-connect to public Wi-Fi on firm devices

Reducing exposure on public networks lowers the chance of accidental disclosure and helps demonstrate reasonable care when handling client information.

Use Outside Help When You Need It

Most firms are not staffed with security specialists, and they don't need to be. What matters is knowing when internal knowledge has limits and bringing in help before problems occur.

- Use outside consultants for initial cloud security reviews
- Validate permissions, access controls, and sharing settings
- Review backup and disaster recovery configurations
- Test incident response readiness before a real event

A short, targeted review can uncover misconfigurations and gaps that are easy to miss internally and much harder to fix after an incident.

Put Security Obligations in Writing

Technology settings can change. Contracts define expectations when things go wrong. Written obligations help ensure your vendor's responsibilities align with your ethical duties.

- Require confidentiality and data protection obligations
- Define baseline security standards in the agreement
- Include breach notification timelines and procedures
- Address data ownership, return, and deletion
- Confirm enforceability of terms

Clear contractual terms reduce uncertainty, strengthen accountability, and support your firm's ability to respond quickly and appropriately if an issue arises.

Train Staff and Set Clear Usage Expectations

Most cloud security incidents start with normal user behavior: clicking a link, sharing a file too broadly, or reusing a password. Training and clear

expectations reduce these risks more effectively than technical controls alone.

- Provide basic security awareness training for all staff
- Cover phishing, password hygiene, and safe file sharing
- Document acceptable use for cloud tools and devices
- Reinforce expectations during onboarding and role changes
- Remind staff how to report suspicious activity

Well-trained staff make fewer mistakes and respond faster when something looks wrong, which helps limit exposure and supports your duty of supervision.

Manage Devices and Remote Work Securely

Cloud access often extends beyond the office. Laptops, phones, tablets, and cloud-based software for remote use can become entry points to client data. Managing those devices is part of managing risk.

- Require full-disk encryption on firm devices
- Enable remote wipe for lost or stolen devices
- Keep operating systems and software updated
- Separate firm data from personal apps when possible
- Review access when devices are replaced or retired

Strong device controls help protect client information even when hardware is lost, stolen, or used outside the office.

Put Secure Cloud Workflows into Practice

Cloud tools can be safe or a source of risk for law firms. The difference is control. When you choose the right vendor, set clear permissions, train your team, and put expectations in writing, you reduce risk and stay aligned with your ethical duties.

When law firms need secure cloud access to the systems that keep work moving, they turn to TimeSolv. Built specifically for legal time tracking, billing, project management, and client collaboration, TimeSolv gives firms anywhere access with practical safeguards that support ethical cloud use.

Ready to see how TimeSolv makes it easier to protect your data in the cloud? Start a free trial now or schedule a demo today.