Why Law Firms Need Role-Based Access Control

Law firms are ethically obligated to protect their clients' data. Any information a client shares with their attorney should remain confidential. However, a cybersecurity attack can compromise the client's private information, allowing hackers to leverage this data for financial gain. Role-based access control can help avoid the fallout of a worst-case scenario situation.

A cybersecurity incident can harm your clients' reputations and finances and negatively affect your firm. Clients can pursue a legal malpractice lawsuit against you, and you could lose cases once prospective clients learn about the data breach.

Your law firm can avoid these negative consequences by implementing a role-based access control policy so it can protect the valuable information clients trust you to keep private.

Data Security for Law Firms

The American Bar Association (ABA) sets rules law firms must follow when it comes to privacy and security standards. For example, according to Rule 1.6:

- Lawyers cannot give away a client's information without the client's informed consent.
- An attorney can reveal a client's information only if the lawyer believes it is reasonably necessary, such as to prevent bodily harm, stop the client from committing a crime, or obstruct financial injury.
- Lawyers must make efforts to prevent unapproved access to client information.

The ABA's Formal Opinion 483 outlines how law firms should handle data security breaches. Per the ABA, lawyers must:

- Take security measures to protect the client, especially when it comes to technology
- Regularly monitor their plans for minimizing the fallout if a cybersecurity attack occurs
- Stop a data breach and prevent a hacker from further releasing client data
- Inform clients of a data breach as soon as possible

Certain sensitive client information may require more than the standard level of security. Because lawyers are often responsible for handling money that belongs to clients, law firms should take extra precautions to protect their clients' financial interests against cyber risks. If a hacker gains access to your firm's Interest on Lawyers' Trust Accounts (IOLTA), you and your client may be in financial trouble.

Taking steps to protect your clients' information, such as by setting up role-based user access, can give your team peace of mind that secure information is protected.

What Is Role-Based Access Control?

Role-based access control limits the access certain team members have to information and system functions based on their role within the firm. Essentially, role-based access control helps keep data secure by ensuring employees can access only the information they need to perform their jobs.

Your firm can delegate access to information based on a few factors, including:

- **Authority.** Lower-level employees may not need access to the same information as your firm's executives.
- **Responsibility.** Employees only need to access information related to their position's duties.
- **Job competency.** Employees whose jobs require more technical skills may need to access certain information.

Your firm can also decide which role each employee should have. Many organizations assign roles like the following:

- **Administrator:** An administrator generally has high-level access to information. Administrator roles are usually assigned to executive employees or members of your firm that need access to certain data to adequately perform their jobs. They can create and edit documents and create and add new users.
- **End user:** These users typically can access information that administrators deem necessary. They may be able to view certain documents but do not have permission to edit or share them.

By implementing role-based access control, you can decide what permissions each user has. For law firms, access management has several uses, including:

Mitigating Cybersecurity Concerns

If your law firm has several employees, each user is likely working on a different device. If your firm's employees work remotely, limiting certain users' access to data can help prevent a data breach.

Many firms also use cloud-based software, allowing their employees to access data, software, and servers using the internet. While this is often beneficial in terms of cost and convenience, allowing users to access information anytime, anywhere presents security concerns. Restricting user access to data stored in the cloud can minimize the risk of compromising sensitive information.

Abiding by the ABA's Rules

As previously mentioned, the ABA requires lawyers to prevent unauthorized access to client information. If your firm allows only high-level employees access to sensitive information, it adheres to the ABA's rules.

Ensuring Law Firm Productivity

Allowing your firm's members to access only the information that is essential to their role can benefit your organization's productivity. Overall, it helps ensure your employees stay on task and focus on their position's goals.

The Importance of Role-Based Access Control for Law Firms

Regularly monitoring access rights is the best practice for ongoing security. If an employee's role within your firm changes, or an employee is terminated, their access should be adjusted. Generally, when an employee is terminated or leaves your firm, you should prohibit them from accessing any of your firm's data. Ensuring you're aware of all users who can view sensitive information can help your firm avoid a data breach.

A routine security audit may also benefit your law firm. This might include:

- Checking in on database permissions to ensure the right users have access to the information they need.
- Reminding your employees to remain alert when it comes to common potential threats, such as phishing attacks, suspicious links, and spam emails.
- Making sure your IT department has a plan in case a cyber attack occurs.
- Running tests to identify potential weak spots in your law firm's data security.

Role-based access control also ensures your firm is not vulnerable to legal liability or disciplinary action from the ABA. You can protect your clients and law firm by safeguarding the sensitive data entrusted with.

Legal technology can make the process of routinely monitoring user access levels easier. For instance, Bill4Time's data security software can help your firm remain productive and keeps your data protected by:

- Offering 24/7 service
- Using data centers to ensure natural disasters and local outages do not compromise your firm's data or productivity
- Providing your firm with options to customize user access and give temporary access to contracted employees
- Automatically tracking user logins

Using legal technology to protect your firm’s sensitive information gives you one less thing to worry about.

Best Practices for Role-Based Access Controls

The following security practices for role-based access controls may make all the difference in protecting your firm’s data. Consider the following:

Track All Data Access

Recording database logins, information downloads, and the locations of logins can help your firm determine how and when a breach was caused. Some firms adopt a User and Entity Behavior Analysis (UEBA) tool to point out any cyber threats.

Require Your Employees to Use Strong Passwords

Hackers can easily access private information when users create insecure passwords. While many users recycle the same password across multiple accounts, this may make them more vulnerable to a security breach.

You can set up your firm’s systems to deny a password that does not meet certain criteria. For example, you may require users to create strong passwords that:

- Are at least 12 to 14 characters long.
- Use a combination of uppercase and lowercase letters.
- Do not include publicly known dates or names, such as your birthdate or your children’s name.
- Use various numbers and symbols.

Your firm’s employees should also regularly reset their login information for password security.

Add Multi Factor Authentication for Enhanced Security

Adding two-factor authentication or multifactor authentication to the login process makes it harder for hackers to log in to your company’s web portals. Multi Factor authentication typically involves typing in your username and password, then:

- Entering a code sent to your mobile device

- Answering security questions
- Getting login information, such as password keys, sent to your email address
- Verifying that you are a human user via Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) tools

Outlook on Keeping Your Firm’s Data Secure

Applying role-based access control to your law practice management software adds a layer of confidence to your firm’s data security. Restricting access to information based on each employee’s role within your firm can ease some stress your firm might face in keeping secure information safe.

Maintaining the privacy of sensitive information not only benefits your clients but can also help your firm stay clear of malpractice lawsuits and repercussions from the ABA. Your law firm can take several precautions to stay safe from hackers, such as training employees to pick up on their tricky tactics and requiring strong passwords.

Your firm may also consider adapting Bill4Time’s data security technology, which allows administrators to appropriately delegate user access and track user logins. With Bill4Time, you can control which users can access the information they need to complete projects while keeping your firm running smoothly. You can also set user permissions for functions, allow temporary access for contractors, and enable automatic login tracking.