

Secure and Convenient Online Legal Practice Management

by Ajit Dandapani, *President and CEO, PortalSoft, Inc.*

One of the primary goals of a legal practice management system is to turn mountains of paperwork into manageable, searchable files. However, to be useful to a legal practice, this data must be sharable, and that means a system that offers both protection and access. A closer look at the security and collaboration features of various online systems is warranted before making a decision to commit resources.

Security vs. Collaboration?

Foremost among the features law offices desire, beyond the ability to effectively manage data, is a painless way of sharing information with clients, colleagues, and experts, followed by absolute confidence that the system will provide “security”—that is, keep the firm’s data and computers safe.

In the fields of legal practice management in general, and document management in particular, the highest level of access is offered by systems that use **Software as a Service (SaaS)**, or “cloud computing”—in this case, a subscription-basis system/service that is not hosted on a firm’s private computer system or on a single physical offsite server but is instead hosted on a secure network of servers and accessed by web browser. As SaaS technologies have moved from “emerging” to mainstream, they have increasingly been deemed to offer the greatest efficiency and cost savings among practice management options.

Explosive growth in cloud computing technologies over the past few years has resulted in huge advances in how data can be stored and handled. These advances have allowed a number of heretofore intensely privacy-protective industries to securely store and share data over the Internet. Indeed, “online banking” and other financial and investing services are so pervasive that most adults in this country have some knowledge of or experience with them. The medical field, too, is increasingly offering physician-to-physician access to patient medical records and radiology (for patient care continuity), as well as allowing patients to view their own medical records, test results, prescriptions, and appointments. In fact, private practice physicians are increasingly finding it cost effective to maintain their office and medical record systems “in the cloud”.

Most law offices would probably be surprised to find that data management systems offered as SaaS can be more affordable, flexible, and useful (not to mention safer) than past options such as storing electronic files on an in-house mainframe or offsite server. And even as the security is enhanced, the collaboration options multiply, so that numerous *safe* levels of access may be tendered, as needed, without opening document and client files to hacker attacks or breaches of confidentiality.

As is often the case with new technology, the best known legal practice management systems are priced well out of range for the average law firm. However, it is also true that

the gold-plated name brand systems may not actually offer a level of service that is responsive to the needs of a mid-level user and can include features that are seldom used. Fortunately, there are a number of extremely secure “high-end” options that are reasonably priced and functionally responsive to most security and collaboration needs of a small or large law firms.

Defining Your Security Needs

When it comes to security features, a reputable SaaS legal practice management system will, in nearly every case, exceed the security features offered by a firm’s current approach to practice management. The risks and costs of traditional methods are easy to understand: data stored on individual computers or in-house networks are vulnerable to break ins, theft, fire, and/or other physical disasters; a lost or broken laptop could create a crisis of missing information as well as potential security breaches; and the server itself is subject to failures ranging from bugs to breakdowns. There is also a significant cost (and some might add, an emotional toll) to employing in-house or contract Information Technology experts with the requisite knowledge to not only set up a complex system but keep it safe against hackers and viruses and still accommodate non-technical users.

For most small- to mid-sized firm, a SaaS approach offers numerous benefits, depending on the actual features it incorporates. So, once the choice has been made to move to a more modern practice management system, the next step would be to look over the available options, their relevance for the practice, and the relative costs from the various systems providers.

Security Features of the Host Network

By its very nature, the SaaS model demands that the data management system be hosted in a datacenter capable of handling thousands of users. Even in their minimum offerings, such hosts offer a security level that far exceeds what small- to mid-size law firms can afford to implement in their datacenters. Look for assurances that the hosting entity takes its own security and data protection/backup responsibilities seriously (for example, levels of backup and redundancy to account for all imaginable sorts of data failures) and that it does not allow any “offshoring” of data (you want your records and documents protected by U.S. laws). And of course, data should be encrypted for network communication; when reviewing the security offerings of candidate systems, look for the terms Transport Layer Security (TLS) or Secure Socket Layer (SSL). Highly sophisticated hosting networks may offer “active-active” high availability (HA) so that, in the case of a failed computer or information “node” in the network, the information is seamlessly picked up by other nodes and the failure causes no disruption to the user. This is distinct from an “active-standby” (or “active-passive”) configuration.

Disaster recovery (DR) services may also be offered by either the host site or the software provider to protect against whole-site outages (that is, if the entire hosting provider site fails due to an unforeseen “act of god”, a mirror site at a different physical location can be up and running to support customers nearly instantaneously).

Security Features/Options of the Legal Practice Management System

In addition, to safeguard against insider attacks (from employees or others who have access privileges) as well as outsider threats from hackers and various types of physical theft, most systems offer an array of built-in security features. Those frequently offered on the user end include account auto-disable features (for example, shutting a user out after too many failed login attempts); session timeouts (to prevent unauthorized users from resurrecting a session on, say, a stolen laptop); login records and displays (often a “first alert” to administrators and individual account users that unauthorized access may have occurred); and “fine-grained” permissions (allowing users to view only what they need, with no access to, or even knowledge of, other information or options).

Defining Your Collaboration Needs

Any parent of a teenager with her own house key is already well familiar with the problems inherent in sharing access. While your daughter may be entirely trustworthy, her best friend may be sneaking off to raid your medicine cabinet. How nice it would be if access to every room in the house could be limited without the need for an endless series of locks and keys. Even better, what if access could be granted only to necessary locations (hallways, family rooms, sinks, etc.), with off-limits locations (such as the medicine cabinet) not only locked but invisible? A well-designed practice management system offers just this sort of access control for peace of mind (and protection of data).

Collaboration can refer to intra-firm (colleague-to-colleague) or extra-firm (colleague-to-client, firm-to-firm) information sharing. The risks of uncontrolled sharing with a colleague are obviously much lower than with an outside consultant, but very few people ever need to know everything about everything, so look for a system that offers both pervasive sharing of the sorts of information and document access that every employee is likely to need, and fine-grained permissions for limiting access to sensitive data. For example, permissions may be set to allow a colleague to view documents for a single matter, enabling collaboration without requiring potentially sensitive documents to be sent back and forth (and thereby minimizing risk of loss, theft, or mishandling of email or paper files). Secure, limited, read-only, extranet access and traceable document delivery can also improve and strengthen communication between a law firm and its clients, keeping the clients both informed and in touch.

Another major advantage of SaaS-based systems is that, when data is securely stored in the cloud, all authorized members of the firm can see and share it (preferably in real time). In contrast, when practice data is stored “safely” behind a firm’s firewall, access may be restricted to those currently in the office, on the office Local Area Network (LAN).

Portal4Law™

Practices looking for a comprehensive and cost-effective SaaS legal practice management system with great security and collaboration features would do well to look into

PortalSoft, Inc.'s **Portal4Law**[™] version 5. This product, while responsive to the needs of any sized law practice, is specifically designed to offer a high-value solution to the management requirements of small- to mid-sized practices, without the high-end price tag.

Portal4Law's Hosting Network: Rackspace

Portal4Law has contracted with **Rackspace Managed Hosting** [www.rackspace.com] to safeguard our customers' data in an electronic vault, the likes of which is beyond the budget (and, often, the IT capabilities and understanding) of small- to mid-size legal firms. Billing itself as "the world's leader in hosting"—and listing Microsoft, Cisco, and Intel among its clients—Rackspace is a top-level hosting service that includes:

- *Physical site security* – Security guards and IT technicians monitor, protect, and service Rackspace's infrastructure. Public access is strictly forbidden.
- *Two-factor authentication, including biometric hand scanners* – Rackspace data centers are physically isolated from everyone but level-three technicians. All entrances and common areas are monitored 24 hours a day via closed-circuit cameras.
- *Numerous redundant systems/protections, including* –
 - N+1 redundant HVAC (Heating Ventilation and Air Conditioning) systems
 - N+1 redundant uninterruptible power supplies (UPS), with diesel generator backup
 - Redundant, multi-provider, high-speed connections to the Internet.

Also, because the hosting provider is in the U.S. and subject to the laws of this country, there is no offshoring of data.

Portal4Law uses SSL cryptographic protocols to protect communications over all our networks, and our server hosting environment is configured to offer daily disk-to-disk backups of all client data (so that any accidental mistakes can be corrected). In addition, the Portal4Law server is architected to support active-active HA for performance as well as availability. Some of the most common failures are mitigated by using specialized technologies to both avoid service outages and correct failures without taking the service offline. To mitigate the effects of lost Internet connections, for example, our hosting provider uses four different Internet service providers so that traffic can be transparently switched to another provider without affecting end user service. Component failures are less common, but can be covered by offering active-active support across multiple computers so that, again, if one computer fails, the others will pick up the customers and continue to offer the service transparently—an offsite disaster recovery feature that Portal4Law's design easily supports.

Other Portal4Law Security Features

Portal4Law offers a number of security features that protect at the end-user level. These include time/date/computer displays that show the last time/date that a user logged in so

that users can be sure that no one else has signed into their account. The use of “best practices” in picking passwords (use of 8+ characters, upper and lower case letters, and at least one number/symbol) is another protective feature for limiting unauthorized access. Portal4Law is also architected to support an auto-disable feature when a user fails to correctly login to an account as well as a batch data purge feature designed to limit accidental data loss (with deleted records moved into a “trash can”-like concept that requires a purge action to clean out; thus, until the trash can is intentionally purged, records can be easily restored). Conversely, because we do not believe most users want their login sessions to automatically “time out” after being idle a set period of time, no time-out feature is included in Portal4Law.

Administrative functions are tracked by Portal4Law through use of an auditable administrative log of all login activities in the system (logged into the database so that it can be audited to see who used the product and when); the system is also architected to support an auditable change log of all actions performed in the database (so that a postmortem of what transpired in the database with regards to a client or a matter, etc., can be performed). Since a significant amount of data theft or destruction is the result of action by disgruntled employees, Portal4Law is designed to support features that would mitigate the consequences, from multiple-level permissions (which could help to avoid such a scenario) to encryption (to make stolen data difficult to read).

Another form of security, and peace of mind for the contracting firm, is Portal4Law’s account termination batch data export (XML format) capability. This feature allows the customer to export all the data from Portal4Law and terminate the relationship. We think that this feature is important for our customers and provides the flexibility of not being locked down to a software vendor. Our research shows that this capability is not being offered by anyone else in the industry.

Portal4Law Collaboration Features

One of the collaborative features that is also a security feature is the ability to set *fine-grained permissions*. Portal4Law allows users with appropriate privileges to set permissions to read, write, delete, or export for each “object” in the system. An object could be a client or a matter or even a document. When users with restricted permissions log into the system, they only see what they have permissions for and are not even aware of all the other objects. Thus, key users can protect themselves and clients from colleagues who have no need to see beyond their scope of work. Likewise, an outside consultant could log into a company with Portal4Law and be allowed only to view documents for a single matter. This enables streamlined collaboration on matters without risking exposure of potentially sensitive documents or client information.

In addition, Portal4Law offers:

- *Pervasive sharing* -
Allows remote access to and sharing of documents, tasks, calendars, clients, rate schedules, etc., that the client has approved for wide access.
- *Always current, real-time views* –
There is never a need to explicitly refresh a browser screen to be assured all members of the firm are seeing current data. Portal4Law ensures all screens, whether in the foreground or background, are dynamically updated, with clear indication of the update time.
- *Extranet access* –
Administrators can give a firm's clients limited, read-only secure access to a subset of the data under Portal4Law management. The same mechanism is leveraged to provide large-payload document delivery (as opposed emailing large attachments).

A final, and often overlooked, security feature is source code protection. Compared to some of the industry giants we are in competition with, PortalSoft is a small company. As is typical practice for start-up and disruptive technology, and the norm in the software industry, PortalSoft can arrange—upon client request—to place Portal4Law's entire source code and all the build files, binaries, etc., into an escrow account.

Portal4Law: Safe and Convenient Legal Practice Management System

In all, the Portal4Law product offers a wide range of security and collaboration features to meet the requirements of most law practices, and it does so at an affordable price with world-class support. When you look at the details and compare the features, most law firms will find that Portal4Law more than fits the bill.