Legal Technology/Data Security Checklist

Questions to Consider When Assessing Practice Management Software

On a scale of 1-10 (1 not at all, 10 extremely), how comfortable are you (and other members of your firm) with technology?

- If you and/or your colleagues are not "tech-savvy", look for software that is easy to learn and configure.

How many professionals (attorneys, paralegals, support staff) require access to data?

- If multiple persons will be using the software, look for features that enhance collaboration and accountability such as task management, work flows and reminders.
- Do you have safeguards in place to ensure that each member of firm only has access to the data necessary to perform their job?

Do you and your colleagues work remotely?

- Can you access critical information when you're not in the office?
- Can you access data from a mobile device?

Which aspects of your business are you hoping to improve through adoption of a legal practice management system?

- Billing & Collections
- Time entry
- Internal productivity reporting
- Calendaring
- Intra-firm collaboration & oversight of cases
- Secure (encrypted) client/opposing counsel communications
- Back up, storage and organization of documents/emails
- Automated workflows

Review, if any, platforms you are currently using for the following:

- Legal Practice Management
- Document Storage/Management
- Backup/Disaster Recovery
- Email
- File Sharing (e.g. Dropbox, Box)
- Hosted Applications (e.g. Office 365)
- Calendar/Docketing
- Time Keeping/Billing
- Accounting Systems
- Project management/workflow
- Other applications

How much are you spending annually on software applications?

ARE YOU INTERESTED IN CONSOLIDATING THESE APPLICATIONS INTO ONE, COMPREHENSIVE, CLOUD-BASED APPLICATION?

Questions to Consider When Assessing Data Security

☐ Are you using cloud-based applications for storing and managing client data?

- The cloud allows you to store and access critical information on a network of servers hosted on the Internet rather than a local server. In case of a disaster, the cloud will deliver a quicker recovery of important information.

☐ Do you use a secure portal to share confidential documents with clients and other third parties?

- Email is not always the most secure means of sharing sensitive information. A client portal will allow your firm to send and receive confidential documents and invoices with people outside of your firm without the risk of third party interceptions.

☐ How frequently do you backup your data?

- Regularly backing up your clients' confidential information should be a part of your firm's daily routine. Backing up your data weekly on a Sunday night could cause a problem if your server crashes on a Saturday. Cloud-based practice management software applications are designed to backup data hourly, 365 days a year.

☐ Can you monitor firm-wide activity relating to matters to prevent security breaches?

- Technology that provides an uneditable, firm feed that keeps you apprised of all matter-related activities will point out when something just doesn't seem right.

☐ Do you know when and how to send encrypted emails?

- Encrypted emails should always be sent when the content contains privileged or highly sensitive information if it were to be intercepted by a third party. Send such emails using an email encryption service, such as RPost.

☐ Is your data stored in state of the art, highly secured data center with network firewalls and multiple locations?

- Most small law firms do not have the technical or financial resources to employ sophisticated security measures with multiple redundant backups. Reputable legal technology companies that utilize Amazon Web Services (AWS) or other leading cloud companies benefit from infrastructures designed to meet the requirements of the most security conscious enterprises.

☐ Is your mobile application secure?

- When storing client information on your mobile app, make sure that you use touch ID authentication so that if your phone is lost or stolen, this information cannot be accessed by anyone else.

☐ Do you utilize court-admissible proof of delivery, time and email contents?

- It is not accurate to assume that an email was delivered because you didn't receive a bounce back. With registered email technology, you can view a delivery audit trail and remain sure that your information was received by the intended party.

Want to learn more? **Contact a practice management consultant at Zola** to schedule a demo of Zola Suite.