XIRA Law

Client Data Security

is your digital environment secure?

Solo practitioners and small law firms have relied on physical security to protect practice and/or client data due to the fact that most records and documents were paper-based and could be locked securely in file cabinets in offices. Fast-forward to 2020. In the age of remote working - storing, sharing, or moving data has become more digitalized and prone to data breaches. This change demands a new approach to security considerations and scrutiny of the latest legal technology.

Client data security is paramount for legal professionals and their clients. Similar to healthcare data, legal information is some of the most confidential data collected. Since clients entrust their attorneys with their most private and sensitive information, they expect it to be kept secure and protected from hackers and ill-intentioned criminals.

With the introduction of legal tech tools to improve practice efficiencies and automation, many attorneys find themselves using multiple, independent applications on their laptops or in the cloud to manage their practice such as:

- Scanned documents
- Email systems
- Text messages
- Video communication (e.g. Zoom and MS Teams)
- Public cloud storage (e.g. Dropbox and Box)
- Financial applications such as Quickbooks
- Practice management software like Clio or MyCase
- Payment systems (e.g. Stripe or Square)
- And finally, traditional paper copies

Fragmented legal data is constantly being stored and transferred from one place to another. This means the risk of client data becoming compromised substantially increases when it is scattered across multiple platforms and moved from one of these applications to another.

letting go of cloud fears

Is there a lot of apprehension to placing client data on the cloud? Certainly. But this is changing as law firms' unwillingness eases and firms begin to experience the efficiencies of cloud-computing. In fact, the ABA's "Legal Technology Survey Report" released in October 2020 found only 13% of attorneys at small firms and 11% from 100+ attorney firms used cloud-based practice management software. This significant contrasts with LogicForce's "2021 Law Firm IT Scorecard" released just a few months later in January 2021 indicating 61% of small to medium sized firms are now using legal-specific practice management systems with cloud capabilities.

Larger legal firms have had the privilege of dedicated IT systems and staff to maintain a secure environment for their legal data. However, solo practitioners and small firms don't necessarily enjoy the same luxury. For these small, legal industry entrepreneurs, worrying about how to cost-effectively implement a robust security solution is a daunting endeavor that can be significantly reduced by identifying potential data security gaps and how to minimize or eliminate them.

What are the data security risks for attorneys?

Below are areas firms should investigate when looking for data security vulnerabilities.

- Client Communication (email): Client communication can be compromised due to phishing emails. Phishing refers to any attempt to obtain sensitive information such as usernames, passwords, or financial details (often for malicious reasons) by impersonating a trustworthy entity (such as an attorney) in electronic communication.

- Client Communication (mobile phone): Client-related text messages, use of unencrypted email, or working on public WiFi networks could leave sensitive data exposed. This information can be hacked by cybercriminals and could be used to gain access to other systems where more sensitive information is stored.

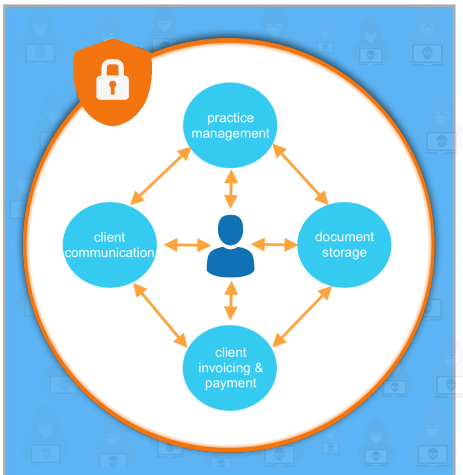
- Client Communication (laptop): Ransomware installed on laptops enables hackers to encrypt files, preventing access to client and practice data, and then demand large sums of money to restore access.

- Social Media: The wide-spread use of social media and online applications has also lead to public breaches of personal and business information. According to the 2019 ABA Cybersecurity Tech Report, 26% of law firms experienced some form of data security breach. Of course, no firm wants to become part of that statistic.

- Multiple, Independent, Applications: When using multiple legal and business applications, sensitive data is fragmented and scattered across many platforms, leaving digital breadcrumbs. As data passes between various systems, it leaves some information behind creating an environment where security can be compromised on other systems.

Minimizing or eliminating security considerations

There are number of easy, inexpensive, and effective recommendations that would reduce or eliminate security risks for client data.



centralized suite of legal tech tools provides most secure environment for law firms

have questions?
if you have questions or need to speak with someone, please contact us at info@xira.com.

XIRA Connect, Inc.
228 Hamilton Avenue, 3rd Flr
Palo Alto, CA 94301
xira.com

rev. a 2/21

1. Solos and small firms should consider using the cloud instead of running legal tech applications on their computers. Cloud environments are typically up to date with the latest security releases and implement encryption, disaster recovery, and backup procedures.

2. Instead of using various applications to manage each aspect of a firm's operation, legal entrepreneurs should switch to a cloud environment with an integrated suite of tools. This helps eliminate fragmented data being moved across multiple systems and applications; thereby reducing the vulnerability of practice and/or client data to cybercriminals.

3. All client communication should occur within a secure, encrypted environment. Do not store documents, process client invoices/payments, conduct video conferences, email, and text message sensitive client data using public, unprotected networks.

4. Setup two-factor authentication whenever available to gain access to accounts and applications.

5. Read all security-related communication from a firm's internet service provider and follow any recommended procedures and software upgrades.

The hybrid working model attorneys experience these days, coupled with a heightened awareness to reduce data security risks for their firm, demands a new approach to traditional security methods. One approach that is growing in popularity is the use of legal services cloud-providers that have a centralized suite of legal tech tools and mobile access. For example, XIRA's GAVEL platform provides an end-to-end integrated solution, so client data never has to be moved or shared between different applications.

As price points lessen and efficiencies firms experience with cloud-based solutions increases, along with continual improvements in practice/client data security measures, we will see a positive upward trend in law firms implementing legal services cloud-computing that provide everything a firm needs to manage their practice in one centralized platform.

get XIRA's free mobile app now!

Download on the App Store

ANDROID APP ON Google play

stay current with XIRA's latest activities and media coverage. check out our press page and like and share our social media pages.