# CONSIDERATIONS FOR SELECTING CLOUD-BASED SOFTWARE FOR YOUR LAW PRACTICE

You may use a variety of software at your law firm. This checklist will help you compare and contrast the security and features of software and know what questions to ask during a software demonstration. For more tips, Practice 2.0's Law Practice Hotline is always available at: (602) 340 – 7332.

**Protecting Your Data**

Multi-factor authentication is a protocol that requires not only a username and password but another piece of information, commonly a verification code texted to your mobile device. This adds another layer of security and minimizes the risk of unauthorized access using your log in credentials.

- ✓ Does the cloud provider offer multi-factor authentication?

    YES        NO

- ✓ Does the provider have a firewall?

    YES        NO

✓ What steps has the provider taken to secure their servers?

_____

_____

_____

✓ Is your data stored on multiple servers?

YES        NO

✓ Is the data you are storing on the cloud safe-harbored, i.e. stored securely by a third party in case of data loss?

YES        NO

✓ Can you maintain your own copy of the data that you store with the cloud provider?

YES        NO

✓ Are there security audits by a third party?

YES        NO

✓ If yes, how often are the security audits?

Frequency: _____

✓ When was the last security audit? _____

_____

✓ What were the results of the last security audit? _____

_____

## Encryption

**Encryption is the process of coding information in a way that only authorized people can decrypt and read it.**

- ✓ Is your data encrypted by the cloud provider?

  YES          NO

- ✓ Is the data encrypted in transit (from your computer to their servers and back)?

  YES          NO

- ✓ Is your data encrypted at rest (while it is on their servers)?

  YES          NO

- ✓ Who holds the decryption key, the provider or you?

  PROVIDER          LAWYER

- ✓ If there is insufficient encryption, are you able to add your own using software you select for that purpose?

  YES          NO

- ✓ If you will be adding additional encryption, what provider will you use?

  Provider name: _____

## Data Ownership and Control

**Who ultimately controls and owns your data?**

- ✓ Where is your data located?

  Server location: _____

- ✓ What laws govern your data?

  _____

_____

✓ Does the provider take ownership in any of your data that it stores?

YES     NO

✓ How does the service respond to third party requests for data such as from the government or other parties? _____

_____

_____

✓ Does the provider store each individual user's data separately?

YES     NO

✓ In the event of a third party or government request for data, would the service be able to pull only the requested party's data (targeted) or would everyone's data (broad) using the service be pulled?

TARGETED     BROAD

✓ Are you able to receive a copy of your data in the event you choose not to use the provider anymore?

YES     NO

✓ In what format is your data provided in that circumstance? _____

_____

✓ If you cancel the service, does the provider keep a copy of your data?

YES     NO

✓ For how long? _____

<u>Data Accessibility</u>

**Data Accessibility refers to your ability to access your data as well as questions about what happens if access points go down and your data is inaccessible.**

- ✓ How can you access the software?

  - ☐ Downloaded directly to the computer

  - ☐ From a computer web browser

  - ☐ From a mobile optimized website

  - ☐ Android app

  - ☐ iPhone app

  - ☐ Client portal

- ✓ Are these alternate methods of access secure?

                    YES          NO

- ✓ Is your computer secured with a password?

                    YES          NO

- ✓ If your computer is lost or stolen, can it be remotely wiped?

                    YES          NO

- ✓ If you can access the service through a smartphone or mobile device such as a tablet, do you have a password on your phone?

                    YES          NO

- ✓ If you can access the service through a smartphone or mobile device such as a tablet, can you remotely erase your phone if it is lost or stolen?

YES          NO

✓ If there is a client portal, have you informed your clients about
appropriately safeguarding their log-in credentials?

YES          NO

✓ If there is a client portal, have you informed your clients about multi-factor authentication (if available from your cloud provider?)

YES          NO

✓ Does the provider guarantee that the service will be functional for a
certain percentage of the time?

YES          NO

✓ What precautions have you taken in case the provider has an outage or
goes out of business? _____

_____

_____

## Security Breaches

**How does the provider handle security breaches?**

✓ Will the provider inform you if there has been a data security breach?

YES          NO

✓ What is the process that the provider takes to inform users of such a
breach? _____

_____

_____

✓ Does the provider indemnify you in case of data loss or a breach?

YES        NO

✓ Does your insurance cover such a loss?

YES        NO

✓ If the data protection offered is insufficient, are you able to enter into a data protection agreement with the provider?

YES        NO

## **Reputation**

What do you know about the provider?

✓ How long has the provider been in business? _____

_____

✓ Does the provider seem well capitalized?

YES        NO

✓ Has the provider previously worked with lawyers?

YES        NO

✓ Was the product developed with consideration given to the professional, ethical, and confidentiality requirements specific to lawyers?

YES        NO

✓ Have you been able to identify any risks with using this application? You might consider doing an internet search for reviews.

YES        NO

✓ Has the provider been the victim of any major security breaches?

YES        NO

## Other Practical Considerations

- ✓ Have you read the provider's service level agreement?

  YES          NO

- ✓ If, after reviewing the *service level agreement*, the provider makes changes to it, to what extent will they inform users of those changes?

  _____

  _____

  _____

- ✓ Have you read the provider's privacy or confidentiality agreement?

  YES          NO

- ✓ Is the provider's service HIPPA compliant?

  YES          NO

- ✓ If, after reviewing the *privacy or confidentiality agreement*, the provider makes changes to it, to what extent will they inform users of those changes? _____

  _____

  _____

- ✓ Are your clients aware that you store your data on the cloud?

  YES          NO

- ✓ Does the service integrate with other providers that your law firm uses?

  YES          NO

- ✓ What hours and days is the service available? _____

  _____

- ✓ What hours and days is technical support available? _____

  _____

- ✓ When does the provider conduct maintenance on its site? _____

  _____

- ✓ What notice does the provider give when maintenance is going to be

  performed? _____

  _____

- ✓ In what format is technical support available?

  - ☐ Online materials

  - ☐ Live chat

  - ☐ Phone

  - ☐ Email

  - ☐ In person training

  - ☐ Videos

  - ☐ Webinars

  - ☐ Other: _____

    _____

- ✓ Can you operate your business if the provider's service goes down?

    YES            NO

- ✓ If no, what is your back-up? _____

  _____

✓ If edits are made to items stored, is there a modification history (such as data modified, last modified by, etc.)?

<div align="center">YES          NO</div>

✓ What is the cost for using the provider? _____

<div align="center">ANNUALLY      MONTHLY      OTHER</div>

✓ What is the onboarding cost/cost for starting the service? _____

_____

✓ Is there a charge for technical support?

<div align="center">YES   NO</div>

✓ Is your data mined such as for advertising purposes, location tracking, etc?

<div align="center">YES   NO</div>