NJSBA
PRACTICEHQ
PREPARED BY
Affinity
CONSULTING

ENCRYPTION OPTIONS FOR ONLINE SYNC PROGRAMS AND PORTABLE MEDIA

ONLINE SYNC TOOLS

It seems like everyone has an online sync program these days. If you're in the Microsoft camp, you have OneDrive. The Google camp has Google Drive. Apple has iCloud Drive. And, Dropbox, the granddaddy of online file sync, is happy to take your money irrespective of your platform choices.

One thing to keep in mind about all these online sync platforms is that a tradeoff exists between convenience (My files everywhere I am!) and security (My files are "up there" in the cloud.). Every major sync service says, and it's true, that your files are encrypted in transit from your device to their servers and back. They also tell you that your data is encrypted at rest, *i.e.*, while stored in their data center. For legal professionals, the concern with both scenarios is that vendor holds the keys to your data. If Dropbox or OneDrive is served with a subpoena or lawful warrant, they can turn over readable data to the requesting party.

A few sync services carved out a niche where you, as the end user, define a password that encrypts your data. If one of these services is served with a warrant or subpoena and they turn over your data, the receiving party still needs the password that only you know to turn the encrypted data into readable information. Sounds nice!

What you lose in the process is most of the integrations between sync services and third-party programs, particularly on mobile applications. One of the reasons some folks refer to Dropbox as the "file system for the internet" is that developers have integrated it deeply into their own programs. Even Microsoft has done this; you can open files from Dropbox in the native iOS Word, Excel, and PowerPoint programs. You don't even need the Dropbox app on your iPhone or iPad to do it.

SECURE YOUR WHOLE CLOUD

If you are comfortable putting your finger on the scale in favor of security and losing a bit of convenience, Tresorit is the cloud vendor for you. They have all the standard cloud sync features, but you can define your own password. They are price-competitive with Dropbox and iCloud Drive. Business plans start at ~$15/user/month.

SECURE A PORTION OF YOUR CLOUD

If you prefer the convenience of Dropbox but want to encrypt a portion of your cloud storage with a password only you know, there exist a couple of encryption programs that "ride on top" of OneDrive, Dropbox, etc. The advantage of these programs is that they only encrypt with your password the individual files or folders you select. If you want most of your sync storage unencrypted, for convenience, but need a portion of "high value documents" encrypted, for security, these cloud sync value-added programs permit this. These services will effectively eliminate your ability to share files with individuals outside of your office, but they also provide complete protection for your files as they are encrypted before the sync service ever gets your files.

- Cryptomator: See https://cryptomator.org. Cryptomator is open-source software that you use to create a special folder called a "vault," which holds files like any other folder on your computer. That vault is password-protected with a password only you know. The vault can be stored anywhere, including the major cloud sync services.

EXTERNAL HARD DRIVE AND FLASH DRIVE ENCRYPTION

If you're uncomfortable with cloud sync storage, or you need to move a large amount of data, if the data requires encryption, then there are a couple of different routes to go.

RELY ON SOFTWARE

There are plenty of software packages that will encrypt data for you. Both Windows 11, via BitLocker To Go, and macOS, via Disk Utility, allow you to encrypt an removable media (e.g., hard drive or flash drives) without spending any extra money.

Going this route means that you can use any hard drive or flash drive you have lying around.

EXTERNAL USB HARD DRIVES

If you do not want to rely on software alone, you operate in a mixed PC and Mac environment, or don't know the operating system or computer situation of the data's possible recipients, several vendors make hard drives and flash drives where the encryption technology is part of the drive's physical construction. They usually have a number pad on the device and require entry of the passcode before the drive can even be seen by the computer to which it is attached.

You could also be a "belt and suspenders" person who encrypts the data via BitLocker or Disk Utility on a drive that also has hardware encryption with physical passcode buttons. The technologies do not interfere with each other.

Here are some options:

HARD DRIVES

- Apricorn Aegis Padlock external hard drives; and
- Lenovo ThinkPad USB 3.0 Secure Hard Drives.

FLASH DRIVES

- Apricorn Aegis Secure Key Encrypted Flash Drives; and
- Kingston IronKey USB Flash Drives.

LEARN MORE

Visit Lawyerist's article on small firm file management to learn more about a systematic approach to safe, convenient, and secure electronic file handling.