NJSBA
PRACTICEHQ
PREPARED BY
Affinity
CONSULTING

TOOLS AND PROTOCOLS TO PROTECT CLIENT DATA

Here are some tools and techniques to keep your client data safe.

ENCRYPTION DEFINED

For purposes of this discussion, we define encryption as follows.

> "Encryption is the process of converting data to an unrecognizable or 'encrypted' form. It is commonly used to protect sensitive information so that only authorized parties can view it. This includes files and storage devices, as well as data transferred over wireless networks and the Internet.
>
> …
>
> An encrypted file will appear scrambled to anyone who tries to view it. It must be decrypted in order to be recognized. Some encrypted files require a password to open, while others require a private key, which can be used to unlock files associated with the key."[1]

LAWYERS MUST ENCRYPT LAPTOPS, TABLETS, AND PHONES

DUTY TO PROTECT

If you carry confidential client data on any of these devices, "reasonable efforts" require you to protect it.

> "Not properly protected, laptops and portable media can be recipes for a security disaster. One survey reported that 70 percent of data breaches resulted from the loss or theft of off-network equipment (laptops, portable drives, PDAs, and USB drives). Strong security is a must. Encryption is now a standard security measure for protecting laptops and portable devices—and attorneys should be using it."[2]

COMPUTER ENCRYPTION

If you have a laptop, someone may steal it, or you might misplace or otherwise lose it. You must encrypt the machine if you have confidential client information on the computer. Encryption prevents a thief or finder of your laptop from obtaining any information from the hard drive, even if they remove it and install it in another computer. There are many choices for this type of software, including the following:

- BitLocker – included for free with Windows 10 and 11 Pro;
- FileVault – included for free with macOS (for use on Apple Macs);
- AlertBoot (Windows only);
- SecureDoc Full Disk Encryption – from Winmagic Data Security (for Windows and Mac).

For solos and small firms, we recommend using the drive encryption created by the operating system vendor, BitLocker for Windows computers and FileVault for Macs. Since the OS vendor creates these solutions, they are the least likely to pose a problem for future software updates.

[1] See encryption as defined by TechTerms.com.

[2] "Encryption Made Simple for Lawyers", by David G. Ries & John W. Simek, *GP Solo*, November/December 2012.

Larger organizations with custom needs or firms with managed IT providers may find value in a customizable third-party solution. However, if a firm's attorney or legal support staffer is also the main IT person, stick to BitLocker or FileVault, as appropriate.

SMARTPHONES

All the smartphone operating systems have free encryption built in. If the smartphone offers biometric security, such as a fingerprint reader, TouchID, or FaceID, and you activate it during setup, it is virtually guaranteed that your smartphone is encrypted. Read more about Apple's iOS security here and Google's Android security here. As of this writing, you would have to try to *disable* encryption on a modern smartphone.

TABLETS

Like smartphones, Android tablets and iPads have built-in encryption, likely enabled by default. The linked articles under Smartphones above apply to tablet devices.