TOOLS AND PROTOCOLS TO PROTECT CLIENT DATA:

Now that you know the rules affecting this issue, here are some tools and techniques to keep your client data safe.

A. **Encryption Defined**: For purposes of this discussion, encryption can be defined 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]

B. **Lawyers Must Encrypt Laptops, Tablets and Phones**:

1. **Duty To Protect**: If you are carrying confidential client data on any of these devices, "reasonable efforts" to maintain confidentiality cannot possibly include doing nothing 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

[1] See http://techterms.com/definition/encryption

now a standard security measure for protecting laptops and portable devices—and attorneys should be using it."[2]

2. **PC Encryption**: If you've got a notebook computer, there's always the chance that someone will steal it or that you'll misplace or otherwise lose it. If you have confidential client information on the laptop, then it would be prudent for you to encrypt the laptop. Encryption would prevent a thief or finder of your laptop from obtaining any information from the hard drive, even if they remove the hard drive and install it in another computer. There are many choices for this type of software, including the following:

   a. **BitLocker** - included for free with certain versions of Windows Vista, 7, 8 & 10.

   b. **Mac FileVault** - included for free with OSX.

   c. **SecuriKey Pro** - https://www.securikey.com/

   d. **Symantec Drive Encryption** - http://tinyurl.com/39seow

   e. **AlertBoot** - http://tinyurl.com/63h36wt

   f. **Folder Lock** - http://www.newsoftwares.net/folderlock/

   g. **SecureDoc Full Disk Encryption** from Winmagic Data Security - http://tinyurl.com/4vek6ot

3. **Smartphones**: All of the smartphone operating systems have free encryption built in, you must only enable it. Make sure you do this.

4. **Tablets**: Like smartphones, Android and iOS tablets have built-in encryption that you must simply turn on. Windows tablets may also have BitLocker depending upon the version of Windows installed. Of course, any of the Windows encryption options above would also work (besides BitLocker).

[2] Encryption Made Simple for Lawyers, by David G. Ries & John W. Simek, GP Solo, November/December 2012 - see http://tinyurl.com/znh4jqz