Attachment 4: An Encryption Quick Start Action Plan

[This Action Plan is from Sharon D. Nelson, David G. Ries and John W. Simek, *Encryption Made Simple for Lawyers* (American Bar Association 2015). References are to Chapters in the book.]

An American Bar Association resolution adopted in August 2014 *"encourages private and public sector organizations to develop, implement, and maintain an appropriate cybersecurity program that complies with applicable ethical and legal obligations, and is tailored to the nature and scope of the organization, and the data and systems to be protected*." It covers attorneys and law firms, as well as other businesses and enterprises. An appropriate information security or cybersecurity program is an essential part of compliance with attorneys' duty under ABA Model Rule 1.6(c) to employ "reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client." Encryption of data is a critical component of an appropriate information security or cybersecurity program. (Chapters 2 and 3)

This Quick Start Action Plan outlines the steps that attorneys can take to implement encryption – **starting now**.

1. **Start with the basics for encryption that you are using now or implementing in the future.** (Chapter 5)
    a. **If you need help in implementing encryption, find someone who is qualified to assist you.**
    b. **Protect encrypted data with strong authentication.**
    In many implementations of encryption, access to the decryption key is protected by the user's password or passphrase. Make sure that you have strong passwords or passphrases for encryption you are currently using or you plan to implement in the future.
    c. **Back up data.**
    Like other areas of technology, there can be technical failures with encryption hardware and software. Keep a secure backup of encrypted data, a step that should always be done, even for data that is not encrypted.
    d. **Back up the recovery keys.**
    In some implementations of encryption, a user can back up a recovery key that may make encrypted data recoverable if a user forgets a password or there is a technology problem. Back up the recovery key in a secure place. In mid-sized and larger firms, recovery keys should be managed by IT staff.
2. **Start with the "no-brainer" encryption solutions – encryption of laptops, smartphones, tablets, and portable drives.** (Chapters 5, 6 and 7)
    The Verizon 2014 Data Breach Investigation Report notes that "encryption is as close to a no-brainer solution as it gets" to protect confidential data on lost or stolen laptops and mobile devices. It's not just Verizon, this view is widely held by information security professionals and

government agencies. Review the devices that you and your firm are using – laptops, smartphones, tablets, and portable drives - and make plans to encrypt them as soon as reasonably possible if they are not already encrypted. With many of them, it's just a matter of turning encryption on. Consider encryption and enable it when you add new devices.

3. **Protect confidential documents with encryption – a solution you already have.** (Chapter 11) Confidential documents transmitted electronically or by e-mail should be protected by encryption. Current versions of Microsoft Office, Adobe Acrobat and WinZip encrypt documents when password protection is used. New Jersey Ethics Opinion 701 (April 2006 - over eight years ago) advised attorneys to password protect documents [encrypt them] when they are sent over the Internet. (Chapter 2.) While this form of encryption may not be as secure as some of the other solutions discussed in the book, it is much more secure than no encryption and is immediately available to most attorneys.

4. **Use secure network connections.** (Chapter 8)
Confidential data that is transmitted outside of a secure network should be protected. This requires secure connections between networks and over the Internet. Review the various network connections that you and your firm use and make sure that they are secure. For the Internet, you should use https:// or virtual private networks as a minimum.

5. **Secure your wireless networks.** (Chapter 8.)
Make sure that your law office wireless network and home networks used for client data are protected by WPA2 (Wi-Fi Protected Access 2) [or WPA3] encryption and are securely configured. If you are using an older wireless access device that does not support WPA2, replace it.

6. **Be careful on public networks.** (Chapter 8)
Make sure that you can use a public network securely for confidential data **before** you use it, or avoid using it. Use only secure connections – https:// or a virtual private network.

7. **Implement an encrypted e-mail solution.** (Chapter 9)
It has now reached the point where most or all attorneys should have the ability to use encrypted e-mail, where appropriate, for confidential communications. A basic level of protection can be provided by putting the confidential communication in a password protected/encrypted attachment. There are now a number of easy to use, inexpensive options that are available for securing e-mail, including ones for solos and small firms.

8. **Use encryption in the cloud.** (Chapter 10)
Encryption controlled by the end-user should be the default for confidential data stored in the cloud. End-user controlled encryption should be required for attorneys unless the attorney makes an informed decision that the data is not sensitive enough to require this level of protection or that the cloud service provider will implement and maintain sufficient security controls without end-user controlled encryption. For attorneys, this requires the analysis required by the ethics rules and opinions discussed in Chapter 2, including competent and reasonable measures to safeguard information relating to clients, due diligence concerning service providers, and requiring service providers to safeguard data in accordance with attorneys' confidentiality obligations.