DR. RICHARD FEDERICI, LLC

Dr. Richard Federici
Licensed Clinical Psychologist

COMMUNICATIONS HANDOUT

Each patient has different circumstances which might influence these decisions. To assist you make an informed decision, the following are **some** areas of risks and safeguards for you to consider. You should do more research if security is a high priority for you.

The following is a generalized compilation of information from many sources to assist you in making an informed decision, and may not address your specific situation.

The most likely vulnerable privacy issue for most people is if their phone, computer or tablet is lost, stolen, or recycled, so sufficient precautions should always be taken in that regard. Text messages often can be accessed without any level of authentication, meaning that anyone who has access to your devise may have access to all text messages without the need to enter a password. Emails or text messages that remain on devices indefinitely can also be exposed in those situations. Using an unsecured public wi-fi hotspot presents a dangerous vulnerability to your security essentially exposing your email account, and password, to anyone with a little technical knowledge. Devises can be hacked and your emails and or text messages may be compromised. Even if you think your devices are secured, someone with access to your phone or computer can use an application which gives them remote access to your devise. The carriers you choose and the specific cell phone manufacturer and model you use also determine vulnerability levels. Service provides keep records of your phone calls, text messages, data usage and pictures sent or received but they do not see the actual messages or photos, however, when a recipient of a text message has their phone powered off, or is out of range, those texts do remain on the providers server making them vulnerable, until they are delivered. Apple claims their iPhones running iOS 8 and later are protected with strong encryption that even they cannot decrypt, rendering it useless to anyone who might get a hold of it, legally or otherwise. Encryption jumbles the content of a message into random symbols and characters until it is received on the other end where the original message is recompiled. Encryption addresses security of the transmission of texts from one device to the next while communicating, but not if you back up that same information to their servers. Backing up devises online to your provider, or to such services as iCloud, gives those providers access to your private information. Backups can be de-coded, and they can turn those records over to law enforcement agencies. Law enforcement officials can wiretap land lines and cell phone lines. Emails that are left on web servers for over six months, are considered ‘abandoned’ and law enforcement and government agencies are able to request those emails without obtaining a subpoena. Should a prosecutor bring a case to trial, and any of those records are submitted as evidence, it could be made public. Unlike confidentiality of medical records such as lab results, or a medical diagnosis, psychological records can be more damaging if they are in the wrong hands. It is impossible to safeguard against the endless possibilities of scenarios where confidential information can wind up in the wrong hands.

346 Main St
Chatham, NJ 07928
973 533 1208

COMMUNICATIONS HANDOUT (continued)

There are measures that Dr. Federici will take to ensure your privacy, and there are measures that you can also take to improve the security of your private information. As technology advances, so does the risk of jeopardizing confidentiality increase. The following is recommended :

- Have strong passwords on all of your devises (cell phones, computers, tablets and iPads)
- Change your passwords regularly
- Consider using a password manager
- Keep all devises current with the latest updates
- Use firewall where appropriate
- Never use unsecured public wi fi hot spots
- Enable 2 step verification where available
- Check with your carrier to assure that your text messages are encrypted
- Check with your internet provider to assure that your emails are encrypted
- Keep up to date with latest vulnerabilities and how to keep safe
- Check your settings on all devises to see if they can make your devise more secure
- Delete text messages and emails containing sensitive matters
- Never forward emails received from Dr. Federici to anyone else
- Completely delete emails off the web server before they are 180 days old. Deleting emails from your computer or cell phone, may not delete them from the server (depending if you have POP or SMTP mail settings). Log into your email account through a web browser (not an email app or program) and delete emails on there
- To ensure privacy, do not allow texts to be displayed on locked screens
- For Android phones enable Android *Device Manager* which can find your phone remotely, and if needed, can remotely erase the contents of your phone
- For iPhones, turn on *Find My Phone* to help locate a lost or stolen phone. Also turn on *Data Protection* to enable your device to remotely erase all its data if ever needed
- Information on your devises could one day potential be turned against you if someone has access you your devices
- Know who is sharing your wi fi, even at home, because they could compromise your security

YOU ARE WELCOME TO CONTRIBUTE MORE SUGGESTIONS

You play a major role in securing your confidentiality. Keep in mind that the most likely threat to security of your confidential matters is the loss, theft, or recycling your phone, so take protective measures accordingly. Part of being vulnerable is not thinking of all contingencies. If you become aware or suspect a breach or vulnerability in Dr. Federici's plan as outlined, you are requested to bring it to Dr. Federici's attention immediately. Security requires procedures to continuously evolve, and Dr. Federici will continue to improve his policies on protecting patient confidentiality