CONFIDENTIALITY - PRIVACY - SECURITY

A JOINT DECISION

Dr. Federici is an advocate for preserving patient privacy and will protect your confidentiality and security. Confidentiality refers to the principal that information is not disclosed to unauthorized people. Information that you confide to Dr. Federici is recognized by law as privileged information, and is confidential. Security refers to the means of protecting your private information to assure that it remains confidential. This practice does not fall under the criteria for HIPAA, and though Dr. Federici is not obliged by law to follow HIPAA protocols, this practice is committed to protecting your confidentiality. Dr. Federici will not disclose any information about you, without your consent, or acknowledgment, which may be via signed forms, or by other acceptable means. The exception to confidentiality is if you are a danger to yourself or others, or in cases of abuse. If you are involved in a life-threatening emergency and Dr. Federici cannot ask your permission, Dr. Federici will share information if he believes you would have wanted him to do so, or if he believes it will be helpful to you. Dr. Federici will take precautions to minimize the risk of disclosing any information about you that you do not want disclosed.

To ensure confidentiality, clinical matters should wait to be discussed during therapy sessions. If, however, you need to consult with Dr. Federici between sessions, you need to weigh the security risks involved with communications outside of the office. Communication refers to any contact outside of a session, such as by telephone, cell phone, text message, or email. Any communication with Dr. Federici which is not in-person increases the chance of intrusion of your privacy. New vulnerabilities arise and new threats are always being detected. New operating systems, and updates, may close security loops, but they too are open to new security breaches. It is prudent to keep the devises that you communicate with Dr. Federici current with the latest updates. Providers and manufacturers have begun providing encryption to protect text messages, however, not every provider provides the same degree security.

To address potential threats, Dr. Federici has designed a plan to help secure your privacy. It is Dr. Federici's intention to set up protocols that make each person feel comfortable, secure, and adequately protected. Certain principles will be adhered to for everyone. There are components to communications outside of the office which you will be allowed to choose your level of comfort. Communications include phone calls, messages, text messaging, and emails. The price for safer communication, is more stringent security measures, which may be burdensome to those who do not require it. You can decide the level of confidentiality you want, and Dr. Federici will do his utmost to honor that. Human error is always a potential occurrence, no matter what safeguards are implemented, and should take that into consideration. You can decide if speaking on a landline, or on a cell phone is secure enough for you. You can decide if texting or email communications are secure enough for you. You can also decide if telephones, cell phones, texting, or emails are secure enough to discuss very personal matters which should normally only be discussed in therapy sessions.

There are many factors to consider including what the nature of the communication is, what method of communication will you be using, the device or devices being used, the service provider of those devises, what risks will you be taking including human error should your communications be erroneously sent to the wrong person, what are the consequences if your communications are compromised, to name a few. These factors should then be weighed against the urgency of the communications, and the benefit factors.

Dr. Federici does not accept 'friend requests' from patients or former patients on social network sites such as Facebook, or LinkedIn, nor will he contact you in that manner. Never divulge any information to anyone claiming to be Dr. Federici on any social media site. Psychologist's ethics code prohibits psychologists from soliciting reviews from clients, nor should psychologists respond to them. You may find Dr. Federici's practice on such sites as Yelp, Healthgrades, or other places that list businesses. Some of these sites include reviews that users rate providers. Dr. Federici is not encouraging or discouraging you from doing so, however, you should be aware that using your own name could compromise your privacy, and it

would be prudent if you do use those sites, to create a separate email account, and a pseudonym, so your identity is not associated with Dr. Federici. Dr. Federici will never contact you on those sites, or on any social media. The only way Dr. Federici will communicate with you is via phone, text or email, depending on how you consented to communicate with Dr. Federici.

When communicating with you, Dr. Federici will only discuss matters that will not need to be entered in his psychotherapy notes. Generally, the details of texts will not be put in his notes unless it is a **"notable event"** which is information Dr. Federici would use in whole or in part to make decisions on how to treat you. Usually these would suggest a higher level of confidentially as well. Dr. Federici keeps records on each patient as well as his own separate psychotherapy notes for each person he sees. Dr. Federici does not keep copies of any texts or emails in your records file, however, if there is a significant discussion, Dr. Federici may need to make note of it. If the Communication goes towards a topic that needs to be documented, under most circumstances, Dr. Federici will stop the conversation and advise you to continue the discussion in the office at the next session. If you want to continue the discussion, and Dr. Federici has the ability to do so, and if he thinks it is in your best interest to continue, the conversation will then be considered an "**impromptu session**" which triggers Dr. Federici to take certain actions and you will be charged a pro-rated amount for the conversation. Once it is an impromptu session, you will be responsible for these charges. The only rare circumstance where Dr. Federici will not stop the discussion to remind you of this, is if he feels it would be harmful to you. For those occurrences, he will however take the highest level of security he is able to take under the circumstances. Some examples would be if you were suicidal, if you just experienced a major life trauma, or if in Dr. Federici's professional opinion it would be detrimental to you, if he interrupted you, or did not let you continue.

If you require high levels of security, or are not sure if the measures of security of Dr. Federici's practice are sufficient for your needs, you should discuss this with Dr. Federici. Dr. Federici will do his best to advise you how to preserve your privacy within the parameters of security measures set up for his practice.

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.

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.

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

To assure that your specific needs are met, Dr. Federici requests that you advise him of your preferences for communication such as leaving a message about appointment times. The forms are available in the office or on the website.