Mobile Device Standard

1.0 Overview

This standard defines additional terms and procedures that are important for understanding the proper use of mobile devices.

2.0 Purpose

The purpose of this standard is to provide all users with the appropriate information to abide by the Mobile Device Policy.

3.0 Scope

This standard applies to clients, patients, staff, or individuals external to “Company Name”s who own or operate a mobile device that communicates with “Company Name”s equipment, networks, or data in any way.

4.0 Standard

The following information is based on the Mobile Device Policy, which states that “Company Name”s sensitive data should not be stored on portable computing devices unless there is no other option. The sections below are not meant to guarantee the security of your data, but provide precautionary measures that should be observed.

4.1 General Guidelines

- “Company Name”s sensitive data must not be transmitted via wireless communication to or from a portable computing device unless approved wireless transmission protocols along with approved encryption techniques are utilized
- Don't connect to unencrypted wireless networks
- Don't access web applications containing sensitive information

4.2 Laptops/tablets

- Use TrueCrypt volumes for encrypted data storage
- Use Password protected login
- Use approved anti-virus and anti-spyware software installed

4.2 iPhones

- Enable Passcode Lock
- Use Applications to store files in a password protected files (e.g., Private Data, Fliq Docs or any number of paid applications)

4.3 PDAs/Other Mobile Devices

- Password lock the screen

5.0 Definitions

“Company Name”s Network – Means any network at “Company Name”s facilities or any network that “Company Name”s has setup for any “Company Name”s Client, Contract or Non Contract.

6.0 Revision History