Policy and Procedure: HIPAA/HITECH Compliance
Topic: *Mobile Devices*

Policy Purpose:

Saratoga Bridges has a requirement to protect its information assets in order to safeguard its customers, intellectual property, and reputation. This document outlines a set of practices and requirements for the safe use of mobile devices.

1. All mobile devices are in scope of this policy, whether owned by **Saratoga Bridges** or owned by employees, that have access to corporate networks, data, and systems, not including corporate IT-managed laptops. This includes all smartphones and tablet computers.
2. Exemptions are only allowed when approved by management in writing and where a risk assessment has been conducted and reported to management.

Policy Description / Responsibilities:

Technical Requirements

1. Devices must use current operating systems.
2. Devices must store all user-saved passwords in an encrypted password store.
3. Devices must be configured with a secure password that complies with **Saratoga Bridges**' password policy. This password must not be the same as any other credentials used within the organization.
4. Devices must have installed and properly functioning remote-wipe capable software.
5. With the exception of those devices managed by IT, devices are not allowed to be connected directly to the internal corporate network.

User Requirements

1. Users must only load data essential to their role onto their mobile device(s).
2. Users must report all lost or stolen devices to **Saratoga Bridges**' IT Department immediately.
3. If a user suspects that unauthorized access to company data has taken place via a mobile device they user must report the incident in alignment with **Saratoga Bridges**' incident handling process.
4. Devices must not be "jailbroken" or have any software/firmware installed that is designed to gain access to functionality not intended to be exposed to the user.
5. Users must not load pirated software or illegal content onto their devices.
6. Applications must only be installed from official platform-owner approved sources. Installation of code from un-trusted sources is forbidden. If you are unsure if an application is from an approved source, contact **Saratoga Bridges**' IT Department.

7. Devices must be kept up to date with manufacturer or network provided patches.
8. Devices must not be connected to a PC that does not have up-to-date and enabled anti-malware protection and which does not comply with corporate policy.
9. Devices must be encrypted in line with **Saratoga Bridges**'s compliance standards.
10. Users must be cautious about the merging of personal and work email accounts on their devices. They must take particular care to ensure that company data is only sent through the corporate email system. If a user suspects that company data has been sent from a personal email account, either in body text or as an attachment, they must notify **Saratoga Bridges**' IT Department immediately. HIPAA information that may have been compromised (non-Bridges account) should be reported to the Privacy or Compliance Officer immediately.
11. Photographs taken with mobile phones are prohibited within **Saratoga Bridges** buildings and grounds unless prior approval is granted.