Agreement for Use of Mobile Device

The use of mobile devices represents a significant risk to [Entity]. Mobile devices are prohibited from being used at any [Entity] facility to capture and then transport electronic information outside of [Entity] facilities unless the use of such devices are approved by senior management, the device is secure, and accountability procedures are adhered.

By signing this agreement you agree to:

1. Maintain the confidentiality of [Entity] owned information and provide all reasonable protections to prevent unauthorized disclosure, loss, or use of such information.
2. You are required to keep confidential all information of patients, including that which is disclosed to you, or otherwise comes within your control, and provide all reasonable protections to prevent unauthorized disclosure or use of such information. A breach of this duty may subject you to disciplinary action including, but not limited to, revocation of your access privileges and corrective action may be taken against you.
3. You are responsible to ensure [Entity] and/or patient information is not accessed by anyone whose current professional duties do not require such access.
4. You must not disclose to anyone any access identification information provided you or permit such information to be viewed by any unauthorized persons.
5. You will not store or limit storage of ePHI on your mobile device.
6. You are authorized to store and/or transport [Entity] owned information on a mobile device only in connection with your assigned duties. No other [Entity] and/or patient information may be transported by you.
7. The use of a digital camera to capture pictures of patients and/or proprietary equipment or documentation is strictly forbidden unless the use of this type of device is required to perform your day-to-day activities or is pre-approved by senior management.
8. You are required to safeguard Information stored on your mobile device at all times. The use of strong user authentication, file compression, and/or automatic data encryption to access the data contained on the device is required and you shall not tamper in any way with the configuration established by the Information Systems Department.
9. You will not modify or delete configuration and security software installed by [Entity]
10. You will not leave your mobile device unattended or unsecured. In the event you lose or otherwise find your electronic portable device missing or stolen, you are required to report the loss immediately to the local law enforcement agency where the incident took place; then subsequently make a report to the [Entity] Information Security Officer.
11. You agree to remote wipe or destruction of all [Entity] applications, data and related security configuration.

12. You understand your device will be monitored when connected to [Entity] network.

13. You understand that [Entity] reserves the right to inspect the contents stored on electronic portable devices and delete contents as it deems necessary. In addition such devices may be seized at any time if necessary as related to a security investigation and/or legal hold.

14. You will hold [Entity] harmless if the mobile device is damaged or your personal data viewed.

15. You will retain a copy of the description of the mobile device assigned to you, to include make, model and serial number, so that when necessary a timely report can be made to law enforcement.

16. You understand and acknowledge that [Entity] policies and procedures apply to mobile device use.

Print Assignee’s Name   Assignee’s Signature   Date

Print Assignee’s Name   Assignor’s Signature   Date