Title: CELLULAR/MOBILE DEVICE POLICY	
Approval By: Trauma Trust Management Team	**Date of Approval:** **Effective:** 4/1/2014 **Revisions:** 6/15, 2/18

Scope:

This policy applies to those employees using personally-owned mobile devices for Trauma Trust business and also mobile devices provided by Trauma Trust.

Policy Statement:

Mobile devices can support better health care and more efficient administration in health care organizations. At the same time the use of such devices creates risks to privacy and confidential information including Protected Health Information ("PHI") and other regulatory controlled information. This policy is therefore intended to permit the use of such devices while managing the risks they present.

The use of mobile devices under this policy is a privilege which may be terminated at any time for violation of this policy, or as a sanction for violation of other Trauma Trust policies. Violation of this policy may be grounds for other sanctions as well.

Table of Contents:

I. Mobile Device Security
II. Bring Your Own Device (BYOD)
III. Trauma Trust Provided Devices
IV. Employee Responsibilities Pertaining to Mobile Devices

Policy:

I. Mobile Device Security

a. All mobile devices, regardless of ownership, that connect to Trauma Trust, MHS and FHS health information resources are required to abide by the requirements in this policy and those of the individual hospital systems.
   i. This mobile device policy is subject to change at any time.

ii. Trauma Trust owned devices will be held to the security standards of each hospital system as set forth by their policies. It is the responsibility of each device user to ensure these security standards are followed.

iii. Trauma Trust reserves the right to inspect the contents of any device used for work purposes or used to store corporate data.

iv. A device passcode of at least 4 digits must be enabled on the device at all times with an automatic lock of 15 minutes or less of inactivity.

v. Devices will be set to erase data after 10 failed passcode attempts.

vi. Mobile device operating systems must be kept up to date with the latest version to maintain optimal security. It is the device user's responsibility to perform the OS upgrades.

vii. Jailbreaking, rooting, or otherwise compromising the security of the mobile device is strictly prohibited.

viii. Any mobile device that accesses Trauma Trust, MHS and FHS resources is subject to all applicable policies including but not limited to HIPAA policies.

ix. Short Messaged Services (SMS) Texting of protected patient health information, pictures, etc. is strictly forbidden unless a secure texting application is provided and then authorized for use by Trauma Trust.

x. Taking pictures in patient areas or of any document or information considered confidential or limited such as PHI or business sensitive is prohibited unless immediately uploading to patient's electronic record.

xi. Mobile devices belonging to Trauma Trust may be manually or automatically wiped in the following situations:

1. Lost/Stolen device.
2. Employment termination.
3. Exceeding maximum allowed attempts to unlock.
4. Compromising device security.

xii. Document attachments in emails must not be saved or exported to any other mobile app or service.

xiii. If using a mobile device to connect to the electronic healthcare record system, absolutely no saving of healthcare information to the device in any format is allowed.

xiv. Trauma Trust may monitor any audit access to corporate resources for the purpose of investigating security breaches and as needed to maintain security and compliance with policies.

xv. Any suspected or actual compromises of security or data, or lost/stolen devices must be immediately reported to the Trauma Trust administrative office.

xvi. Mobile apps may only be downloaded through venues approved by Trauma Trust, MHS and FHS.

xvii. Mobile devices must not be used as a storage device to transmit or move data known as "mass storage mode", enabling the device to be seen as a disk drive on a computer.

xviii. Should the use of a mobile device be used for providing patient care, refer to the MHS or FHS infection control policy for additional requirements.

xix. Sharing of mobile devices is only allowed for Trauma Trust owned devices that are purchased for the purposes of general use such as an on call support. Sharing of other devices is generally not allowed unless explicitly allowed by management.

xx. Failure to follow the rules outlined in this Cellular/Mobile device policy may result in loss of access to corporate and hospital resources as well as disciplinary action, up to and including termination of employment.

II. Bring Your Own Device (BYOD)

a. In addition to the requirements set forth in section I, applicable to all mobile devices, employee owned devices have the following addition requirements outlined in this section.

b. Authorization to use mobile devices:

i. Personal mobile devices used in support of Trauma Trust business or operations are to be used only for the purpose or activity outlined in this policy.

ii. Use and disclosure of information subject to this policy by a mobile device, in any Trauma Trust, MHS or FHS facility or office, including an authorized home office or remote site, must be in compliance with all Trauma Trust, MHS and FHS policies at all times.

iii. Authorization to use a personal mobile device at work may be suspended at any time if the user fails or refuses to comply with this policy.

1. Failure to comply with this policy will result in forfeiture of the monthly stipend for authorized personal devices.

iv. In addition to other requirements and prohibitions of this policy mobile device users have the following responsibilities:

1. Employees must utilize their own support options with their phone and/or service provider.
2. Trauma Trust, MHS and FHS information must be removed before the disposal of the mobile device or transfer of ownership.

III. Trauma Trust Provided Devices

a. In addition to the requirements set forth in section I. applicable to all mobile devices, company-owned devices have the following additional requirements
   - **i.** Personal use of Trauma Trust, MHS and FHS information is strictly prohibited.
     1. This includes any information, including media, collected at a Trauma Trust site, patient information, employee information, financial information or Trauma Trust strategic information.
   - **ii.** Incidental personal use of Trauma Trust devices is allowed as long as personal use:
     1. Is negligible in time consumption and frequency while on service.
     2. Is at no cost to Trauma Trust.
     3. Does not impact Trauma Trust in any way or prevent employees of Trauma Trust from performing their duties.
   - **iii.** Trauma Trust reserves the right to monitor all equipment and usage for appropriateness.
   - **iv.** Trauma Trust provided devices are for conducting Trauma Trust business.
   - **v.** Any Trauma Trust provided device in the possession of an individual must be returned to Trauma Trust by the individual upon completion or termination of position.

IV. Employee Responsibilities Pertaining to Mobile Devices

a. General Expectations
   - **i.** Mobile devices must be stored in a secure location when not in use and protected from theft and or damage.
   - **ii.** Employees are expected to abide by all applicable laws covering the use of mobile devices while in employment of Trauma Trust.
   - **iii.** The phone numbers associated with Trauma Trust provided devices remains the property of Trauma Trust at time of separation.
   - **iv.** The plan, service provider and equipment provided is at the sole discretion of Trauma Trust for all company issued devices.
   - **v.** International dialing is not enabled and should not be used.

1. Should costs be incurred for unauthorized usage, they will be charged back to the employee that incurred such charges via payroll deduction.
2. Exceptions may be granted on a case by case basis.

vi. Lost or Stolen devices will be replaced at the cost of the employee that the device was issued to via payroll deduction.

1. Exceptions may be granted on a case by case basis.

vii. Standard issue items for each company provided device are as follows:

1. Mobile Cellular Phone.
2. USB charging cable and wall plug.
3. Protective case.
    a. Additional accessories may be used on company provided devices at the cost of the employee.