HIPAA-43 Mobile Device Policy

Effective Date:	12-01-2015	Last Revised:	7-17-2017

Scope of Policy

This policy governs the use of mobile devices that can access, use, transmit, or store electronic Protected Health Information ("ePHI") in the custody of **TCS**. All personnel of **TCS** must comply with this policy. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Assumptions

- **TCS** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements at 45 CFR Parts 160 and 164, as amended.
- Full compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties. Possible sanctions and penalties include, but are not limited to: civil monetary penalties, criminal penalties including prison sentences, and loss of revenue and reputation from negative publicity.
- Full compliance with HIPAA strengthens our ability to meet other compliance obligations, and will support and strengthen our non-HIPAA compliance requirements and efforts.
- Full compliance with HIPAA reduces the overall risk of inappropriate uses and disclosures of Protected Health Information (PHI), and reduces the risk of breaches of confidential health data.
- The requirements of the HIPAA Administrative Simplification Regulations (including the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules) implement sections 1171-1180 of the Social Security Act (the Act), sections 262 and 264 of Public Law 104-191, section 105 of 492 Public Law 110-233, sections 13400-13424 of Public Law 111-5, and section 1104 of Public Law 111-148.

Policy Statement

- It is the Policy of **TCS** to extend all the privacy and security protections required by HIPAA to Protected Health Information accessed, used, transmitted, and stored on mobile devices operated by members of our workforce.
- It is the Policy of **TCS** to include privacy and security issues related to mobile devices in our Risk Management process and analyses, to better understand risks inherent in the use of such devices.
- This Policy applies to all electronic computing and communications devices which may be readily carried by an individual and are capable of receiving, processing, or transmitting Protected Health Information, whether directly through download or upload, text entry, photograph or video, from any data source, whether through wireless, network or direct connection to a computer, other Mobile Device, or any equipment capable of recording, storing or transmitting digital information.
- This Policy applies to personally-owned Mobile Devices as well as Mobile Devices owned or leased by, and provided by **TCS**.
- Mobile Devices which cannot be or have not been configured to comply with this Policy are prohibited.
- It is the Policy of **TCS** to limit the access, use, transmittal, and storage of Protected Health Information exclusively to those mobile devices that can be configured and operated to deliver privacy and security comparable to the non-mobile data processing systems and devices that we operate.
- It is the Policy of **TCS** to limit the access, use, transmittal and storage of Protected Health Information on mobile devices to the Minimum Necessary, as that term is defined in the HIPAA Regulations.

- ❑ It is the Policy of **TCS** to train workforce members on the safe and secure usage of mobile devices that are utilized to access, use, transmit, or store Protected Health Information
- ❑ It is the Policy of **TCS** to fully document all mobile device-related activities which involve Protected Health Information, in accordance with our Documentation Policy and the requirements of HIPAA.

Procedures

- ❑ Only company-owned and authorized devices may be used to transmit electronic PHI. Any exception will require specific approval by the Executive Director as well as the employee's acknowledgement of **TCS** BYOD Policy. Any access, use, transmittal or storage of Protected Health Information subject to this Policy by a Mobile Device, and any use of a Mobile Device in any **TCS** facility or office, including an authorized home office or remote site, must be in compliance with all **TCS** policies at all times.
- ❑ Authorization to use a Mobile Device may be suspended at any time:
  - If the User fails or refuses to comply with this Policy;
  - In order to avoid, prevent or mitigate the consequences of a violation of this Policy;
  - In connection with the investigation of a possible or proven security breach, security incident, or violation of **TCS**'s policies;
  - In order to protect life, health, privacy, reputational or financial interests; to protect any assets, information, reputational or financial interests of **TCS**;
  - Upon the direction of the Executive Director.
  - Authorization to use a Mobile Device terminates:
  - Automatically upon the termination of a User's status as a member of **TCS**'s workforce;
  - Upon a change in the User's role as a member of **TCS**'s Workforce, unless continued authorization is deemed appropriate.
  - If it is determined that the User violated this or any other **TCS** policy, in accordance with **TCS**'s Sanction policy.
- ❑ The use of a Mobile Device without authorization, while authorization is suspended, or after authorization has been terminated is a violation of this Policy.
- ❑ At any time, any Mobile Device may be subject to audit to ensure compliance with this and other **TCS** policies. Any User receiving such a request shall transfer possession of the Mobile Device to the Executive Director at once, unless a later transfer date and time is indicated in the request, and shall not delete or modify any information subject to this Policy which is stored on the Mobile Device after receiving the request.