HIPAA-44 Bring-Your-Own-Device (BYOD) Policy

Effective Date:	8-10-2015	Last Revised:	7-17-2017

Scope of Policy

This policy governs the use of personal, (non TCS owned) mobile devices by any member of the TCS workforce to 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.

The purpose of the policy is to develop the appropriate safeguards to protect ePHI and other sensitive data on employee personally owned devices. Proper security controls are essential to protect any sensitive information that may be on these devices. Documented instructions and requirements should be provided to all employees that may be accessing or storing ePHI and sensitive company data on their personally owned devices and acknowledgement of acceptance should be documented and retained.

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 regardless of ownership of the equipment.
- TCS may be responsible for any breaches of ePHI and may suffer consequences of breached sensitive company data that resulted from unsecured employee personally owned devices.
- Employees must be aware that breaches or inappropriate use of their devices that may put ePHI and/or sensitive company data at risk may negatively affect clients, **TCS** and the employee themselves.
- **TCS** has the right to revoke an employee's access to ePHI and/or sensitive company data or levy sanctions laid forth in **TCS**'s sanction policy.
- Encryption of devices usually offers a safe harbor under federal and state regulations and is the strongest protection against a data breach. Encryption should be used on all devices that access or store ePHI and/or sensitive company data.
- Employees are not permitted to access ePHI and/or sensitive company data, on personally owned devices, unless authorized and approved. Only approved devices that are properly configured will be given access to ePHI and/or sensitive company data.

- ❑ **TCS** will limit who has access to ePHI and/or sensitive company data on their personally owned devices. **TCS** will provide employees with only the limited amount of access to ePHI and/or sensitive company data to perform their job function.
- ❑ **TCS** reserves the right to install software that allows it to locate, wipe/erase any ePHI or company data from the personal device in the event that it is lost or stolen, or employee's job is terminated.
- ❑ **TCS** and their Information Technology (IT) service vendor will work together to manage and enforce this Bring Your Own Device (BYOD) policy.

Procedures

- ❑ **TCS** will communicate this policy to their employees. Employees must request permission to use personally owned devices and fill in the registration form provided.
- ❑ **TCS** and IT will periodically review and update this policy when new requirements are implemented or when security requirements change. Employees must be notified of any changes and a document of their acceptance/acknowledgment should be collected.
- ❑ **TCS** and IT reserve the right to monitor and inspect devices registered in its BYOD program to ensure that ePHI and sensitive company data are being properly protected.
- ❑ Upon an employee's termination of employment, **TCS** and IT will ensure that any devices the employee has with ePHI and/or sensitive company data are returned to IT for a final analysis and removal of any ePHI and/or sensitive company data or applications that access ePHI and/or sensitive company data. This will be conducted as soon as possible to limit inappropriate access to ePHI and/or sensitive company data.
- ❑ Documentation, acknowledgement and registration forms will be retained for all employees and kept in their employee folder. Documentation must also be provided to employees initially and upon request.