BYOD Guidelines, Requirements and Restrictions/Limitations

This document provides the guidelines for a Bring Your Own Device (BYOD) policy for **TCS**. It offers principles to help guide employees and staff and can be modified by the company to better reflect their specific needs. TCS employees have the ability to bring and utilize various personal devices that may have the ability to access, store or transmit ePHI and/or sensitive company data. Devices include but are not limited to smartphones, tablets and laptops.

Employees must be aware that when accessing ePHI and/or sensitive company data on their personally owned devices, they must protect that information. The ability for employees to utilize personally owned devices for work tasks should be treated as a privilege and **TCS** reserves the rights to revoke this privilege if an employee does not abide by the policies laid forth.

Security Requirements

- All devices must be password protected.
- Passwords must be complex; requiring a minimum of 8 characters, a combination of upper- and lower-case letters, numbers and symbols. Passwords must be periodically reset based on The Company password policy
- Devices must lock after five incorrect password attempts (if supported).
- Devices must "time out" and require a password after a five minute period of inactivity (if supported).
- Text messages that may contain ePHI and/or sensitive company data must be sent through the secure texting application provided. **If a secure texting application has not been provided then employees should not send ePHI and/or sensitive company data via text.**
- Emails that are sent through the device containing ePHI and/or sensitive company data must be sent encrypted. **If secure email encryption is not provided, employees should not send email that contain ePHI and/or sensitive company data via email.**

Restrictions and Limitations

- "Rooted" or "Jailbroken" devices are not permitted to access ePHI and/or sensitive company data.
- Employees must notify management when selling, trading in, recycling or disposing of their personal devices.
- The employee's device may have data remotely deleted / wiped if 1) the device is lost or stolen, 2) the employee terminates his or her employment, 3) IT detects a data or policy breach, a virus or similar threat to the security of The Company's data and/or technology infrastructure.
- Devices that are lost or stolen must be reported to management and/or IT as soon as possible but within 24 hours.
- Employees must inform management and/or IT if they plan to upgrade, recycle or dispose of their personally owned device.
- Employees who voluntarily resign from the organization must present their device(s) to management and/or IT within 48 hours to have all ePHI and/or sensitive company data and/or access deleted / removed from the device.
    - Employees who do not turn over their device(s) to management and/or IT within 48 hours after voluntary resignation are subject to a full remote wipe / deletion of all data including non ePHI and sensitive company data on their device.
- TCS will prepare for scheduled terminations in advance and ensure that employees present their device(s) to management and/or IT the day of the scheduled termination to have all ePHI and sensitive company data and/or access deleted / removed from the device. Terminated employees that do not present their device(s) will be given an opportunity to bring in their device(s) to have all ePHI and sensitive company data removed from the device(s). Terminated employees that fail to

bring in their device(s), after given the opportunity, are subject to a full remote wipe / deletion of all data including non ePHI and/or sensitive company data on their device.

Sanctions
Violations or abuse of this policy are subject to the repercussions laid out in The Company's sanction policy.

Additional Information

The organization will provide any additional specifications, requirements or restrictions in this section.

Devices Permitted:	
Device Type	**Specific Brands & Models Permitted (if applicable)**
Smartphones	
Tablets	
Laptops *	
Other; (List below)	

- personally owned laptops must be accepted and approved by The Company's management.
- Additional Devices: other additional personal devices that may access or store ePHI must be approved by The Company management and IT.

Devices Specifically Excluded:

Applicable Security Specifications:

Mobile Device Management service:	
Encryption service:	
Anti-Malware/Anti-Virus service:	
Minimum Operating System required (laptop):	
Minimum Operating System required (smartphones):	
Minimum Operating System required (tablets):	
Secure texting application required:	
System Inactivity timeout setting (minutes):	
Email Encryption provider:	

Device Security Specifications (for IT and/or (company name) management to complete):

Security Specification	**Implemented (yes or no)**	**Details or additional information**
Operating system		
Encryption		
Anti-virus service		
Secure Texting Application		
Timeout/lock settings		
Password requirements		
Web browser		
Mobile wipe		
E-mail provider		

Bring Your Own Device – Device Registration / Acknowledgement Form

Device Registration:

Employee name: _____

Position/title: _____

Phone number: _____ Secondary Phone number: _____

Device and Description: _____

_____

Serial Number: _____ MAC Address: _____

Employee Acknowledgement

I have read, understand, and agree to comply with the foregoing policies, rules, and conditions governing the use of personally owned devices that may access, store or transmit ePHI and sensitive company data. I am aware that violations of this guideline of appropriate use may subject me to retraction of this privilege or disciplinary action, including termination of employment. I further understand that inappropriate use of my device that may put ePHI and sensitive company data at risk may negatively affect customers, The Company and myself.

I am aware of the technical restrictions and requirements on my device that were provided in the device registration form. I will maintain and manage these security requirements on my device for as long as I continue to access, store or transmit ePHI and sensitive company data. I understand that The Company reserves the right to protect their customer's information as well as sensitive company data that I may be accessing and therefore have the right to remotely wipe / delete data from my device if the need arises.

By signing this Agreement, I agree to comply with its terms and conditions. Failure to read this Agreement is not an excuse for violating it.

_____ _____

Signature Date

_____ _____

Requestor's Immediate Supervisor Signature Date

_____ _____

Information Technology Provider's Signature Date

Information Technology - Chain of Custody Tracking Form

Custodian Name[1]:				Date:	
Company:				Time:	
Address:					
City:		State:		Zip:	
Phone#:		Vendor Service Ticket#:			

[1] Name of person assuming custody of information technology equipment

Description of Equipment		
Item #	**Qty.**	**Description of Item** (Model#, Serial#)
1		
2		
3		
4		

Item #	**Date/Time**	**Released by** (Print Name & Signature)	**Received by** (Print Name & Signature)

Final Resolution/Release

Item(s) #: _____ on this document was/were released by _____ to

Company Name: _____

Name: _____

Address: _____ City: _____State: _____

Zip Code: _____ Telephone Number: (____) _____

I certify that I am the lawful representative/client/owner/ of the above item(s).

Signature: _____ Date: _____

This Chain-of-Custody form is to be retained subject to TCS HIPAA Documentation Policy