

# HIPAA-16: Access, Authorization, Establishment, Modification and Supervision Policy

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

## Scope of Policy

This policy governs the authorization and supervision (oversight and training) of health data-related access and activities for **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 pertaining to the authorization and supervision of workforce members who will be accessing individually identifiable health information as part of their work-related duties, in accordance with the requirements at § 164.308(a)(3).
- Compliance with HIPAA is mandatory and failure to comply can bring severe sanctions and penalties.
- Proper and appropriate authorization to access individually identifiable health information, and appropriate supervision of workforce members authorized to access individually identifiable health information, are essential components of a well-managed risk management system.
- Proper and appropriate authorization to access individually identifiable health information, and appropriate supervision of workforce members authorized to access individually identifiable health information, can help reduce our overall risk, and reduce the likelihood of data breaches and HIPAA violations.
- Establishing, maintaining, and modifying appropriate levels of workforce member access to individually identifiable health information and Protected Health Information can help reduce the likelihood of data breaches and HIPAA violations.

## Policy Statement

- It is the Policy of **TCS** to only permit workforce members who have been appropriately authorized, to have access to individually identifiable health information.
- It is the Policy of **TCS** to properly and appropriately oversee and train workforce members who have access to individually identifiable health information.
- Workforce members of **TCS** shall have access only to the individually identifiable health information that they need in order to perform their work-related duties.
- The level of access to individually identifiable health information and Protected Health Information granted to each member of the workforce shall be independent of the technology used to access such information, and shall apply to access through a workstation, transaction, program, process, or other mechanism.
- Any workforce member's ability to access individually identifiable health information shall be modified immediately when the nature of their job changes and requires a different level of access, whether greater or lesser.
- Higher levels of access shall be provided only to those who need it.
- Any workforce member's ability to access individually identifiable health information shall be modified immediately when the nature of their job changes and requires a different level of access, whether greater or lesser.
- It is the Policy of **TCS** to fully document the authorization, access establishment and modification-related activities for all workforce members who have access to individually identifiable health information.

## **Procedures**

- Only active employees and approved information technology support vendors subject to BAA will have valid usernames and passwords granting network access to electronic PHI systems.
- TCS** employs a role-based access system, meaning that all individual patient databases will be password protected and contain only those records of individuals required for the employee to perform his/her work-related duties. Such duties may include, but are not limited to, clinical documentation of service provision, oversight activities, peer review or other quality improvement efforts, and coordination of billing activities.
- Clinical supervisors will be afforded access to the database of their supervisees for purposes of supervisory activities and clinical oversight.
- Quality Improvement Members will be granted broader access for purposes of peer mentoring, peer review of clinical documentation, and other quality improvement efforts.
- Appropriate administrative staff will be afforded access to PHI required for billing purposes or other appropriate and required work-related duties.
- In the case of archived paper charts (or other hard-copy PHI), only authorized staff will have access to the keys or codes required to obtain such PHI.
- All staff will be trained at the time of orientation, and annually thereafter, on HIPAA related policies, including the expectation and requirement that employees only access PHI (in any format) that is necessary to perform their work-related duties.
- Quarterly check of Active Directory to ensure all users are still employed.