HIPAA-03: Documentation Policy

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

Scope of Policy

This policy governs the creation and maintenance of HIPAA-related documentation for **TCS**. This involves requirements for HIPAA documentation availability and updating, as well as the retention of all HIPAA records. 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 concerned with documentation at § 164.312(b)(2)(i), § 164.316, § 164.530(j)(1)(ii), § 164.530(j)(1)(iii), at minimum.
- Appropriate and timely updating of HIPAA-related documentation is both a requirement under HIPAA and good business practice.
- Appropriate and timely maintenance of HIPAA-related documentation is essential to proving our compliance with HIPAA, responding to investigations, and to effectively serving our constituents.
- Proper and lawful retention of HIPAA-related documentation is both a requirement under HIPAA and good business practice.
- Proper and lawful retention of HIPAA-related documentation is essential to proving our compliance with HIPAA, responding to investigations, and to effectively serving our constituents

Policy Statement

- Officers, agents, employees, contractors, temporary workers, and volunteers who work for or perform any services (paid or unpaid) for **TCS** must document all HIPAA-related activities that require documentation.
- All HIPAA-related documentation must be created and maintained in written form, which may also include electronic forms of documentation.
- Any action, activity or assessment that must be documented, shall be documented in accordance with this and other policies and procedures implemented by **TCS**.
- All HIPAA-related documentation must be forwarded, used, applied, filed, or stored in accordance with this and other policies and procedures created and implemented by **TCS**.
- All required HIPAA documentation shall be securely and appropriately maintained and stored in accordance with HIPAA Regulations and with **TCS**'s policy on document retention.
- HIPAA documentation shall be made available, as needed, to all workforce members who are authorized to access it, and shall be made available to appropriate authorities for audits, investigations, and other purposes authorized or required by law.
- **Availability -** It is the Policy of **TCS** to make all HIPAA-related documentation available to those persons responsible for implementing the policies and/or procedures to which such documentation pertains.
- All HIPAA-related documentation shall be distributed or made otherwise available to all workforce members who are affected by the documentation, or who require such documentation in the performance of their work-related duties.
- Workforce members affected by specific HIPAA-related documentation shall have access to such documentation prior to their beginning or executing work that depends on such documentation.
- No member of the workforce shall be held accountable for compliance with any HIPAA-related documentation, policies, or procedures unless they have been given access to such documentation.

- ❑ **Updating** - It is the Policy of **TCS** to review all HIPAA-related documentation periodically, and update such documentation as needed, in response to environmental or operation changes affecting the privacy or security of individually identifiable health information.
- ❑ Reviews of HIPAA-related documentation shall be made periodically, but at least every 12 months for the purposes of this policy.
- ❑ Reviews and updates of HIPAA-related documentation that occur as a result of this policy shall be made by **TCS**'s designated Privacy Officer.
- ❑ Reviews and updates of HIPAA-related documentation that occur as a result of this policy shall be documented according to **TCS**'s Documentation Policy.
- ❑ **Record Retention** - It is the Policy of **TCS** to retain all HIPAA-related documentation for a minimum period of six (6) years from the date of its creation or modification, or the date when it was last in effect, whichever is later. This shall include privacy policies and procedures, privacy practices notices, dispositions of complaints, and other actions, activities, and designations that the Privacy Rule requires to be documented. Note: six-year requirement pertains only to documentation required by HIPAA regulations, not to medical records.
- ❑ HIPAA documentation shall be securely stored and maintained in a manner consistent with the HIPAA Privacy and Security Rule Standards.
- ❑ HIPAA documentation shall be made available to those workforce members who have a legitimate need for it, and who are authorized to access it, according to current HIPAA Standards.

HIPAA Documentation includes the following:

- ❑ HIPAA Policies and Procedures.
- ❑ HIPAA Risk Analysis and related notes and research materials
- ❑ Policies and Procedures for minimum necessary uses by our organization.
- ❑ Accounting documentation which include:
  - o information required in any accounting (i.e., dates of disclosures, name of entity receiving disclosures; description, etc.);
  - o the written accounting that is provided to the individual; and
  - o the titles of the persons or offices responsible for receiving and processing requests for an accounting by individuals
- ❑ Amendment documentation, including amendment requests and supplemental material received, such as statements of disagreement and rebuttal statements, approval or denial notices.
- ❑ All complaints received and their disposition, if any.
- ❑ Business associate agreements with service providers and contractors including all contracts and addenda to existing contracts with business associates, as well as amendments, renewals, revisions, and terminations.
- ❑ The name and title of the privacy official and contact person or office responsible for receiving complaints and providing information on the notice of privacy practices.
- ❑ Training provided (i.e., topics, dates, and, ideally, participants).
- ❑ Sanctions imposed against non-complying work force members.
- ❑ All versions of the Notices of Privacy Practices and signed acknowledgments of receipt (if health care provider); and documentation when unable to obtain acknowledgement.
- ❑ The methods and results of analyses that justify release of de-identified information.
- ❑ Agreed-to restrictions on uses and disclosures of information and terminations of such restrictions.
- ❑ Access documentation, including the designated record sets subject to access by individuals; the titles of the persons or offices responsible for receiving and processing requests for access by individuals; access approval/denial notices and requests for review.
- ❑ All signed authorizations and revocations.
- ❑ All approved confidential communication requests and terminations or revocations.

- ❑ Incident documentation for any privacy and security incidents that occur.
- ❑ Breach notification documentation for any breaches that occur.
- ❑ Regulatory compliance correspondence and assessment reports.
- ❑ Physical security maintenance records.
- ❑ Information systems activity reviews, decisions made, and investigations conducted.
- ❑ Log records pertaining to views and updates of ePHI.
- ❑ Contingency plans in effect during the retention period.
- ❑ Contingency plan tests.
- ❑ Change Control Forms (approved)
- ❑ Chain of Custody Records of the movements of hardware and electronic media used to store ePHI, including the receipt of any new hardware or electronic media storing ePHI. This record should contain, at a minimum, the name of the person responsible for the item, the location of the item, and any movement of the item.

Procedures:

- ❑ All HIPAA documentation will be identified and categorized to facilitate document retention and availability.
- ❑ HIPAA documentation will be stored in appropriately secured and environmentally controlled facilities. This shall include both physical documents and electronic documents.
- ❑ The names of the agency's HIPAA Privacy and Security Officers will be conspicuously posted in **TCS**'s waiting room. This information will also be included in the agency's HIPAA Notice of Privacy Practices, which is contained in the client orientation packet.
- ❑ Each client is asked to sign and date a Receipt of Acknowledgement of **TCS**'s HIPAA Notice of Privacy Practices. This completed document, when received in our office, will be scanned and stored in accordance with our data retention policy.
- ❑ Training on HIPAA Policies and Procedures is provided at the time of new hire orientation, and annually thereafter at the agency's All Staff Training, which occurs every June. Following each training, all employees will be asked to sign off on a Training Verification Form, which is retained in the employee's personnel file.
- ❑ HIPAA Policies and Procedures are contained in a binder that is stored in TCS's central administrative office. In addition to remaining available in the administrative office, HIPAA Policies and Procedures will be electronically distributed via an agency wide email once per calendar year.
- ❑ Monthly minutes from the HIPAA Committee meetings will be stored in a binder in TCS's administrative office.
- ❑ Record Release Tracker is an electronic database containing a record of all Protected Health Information that has been released by the agency. It details by whom the request was made, provides verification that proper authorization has been granted, and indicates to whom the information was provided, as well as the date of the disclosure. All information contained in Record Release Tracker will be retained in accordance with our data retention policy.
- ❑ The HIPAA Privacy Officer will review the status of HIPAA-related documentation annually.
- ❑ Updated versions of HIPAA-related documentation will be made available to all employees as appropriate.
- ❑ **Record Retention** - Hard copies of client mental health records and other documents containing PHI will be stored in locked filing cabinets for the duration of the document retention policy. No hard copy documents will be destroyed without verifying compliance with this policy.
- ❑ Data backup system will be implemented with appropriate backup job schedules and electronic data retention policies for ePHI to comply with this policy.