TCS, Inc.

The Counseling Source Inc.
On-site Mental Health Services

HIPAA Policy and Procedures Manual

HIPAA
Health Insurance Portability & Accountability Act

Date: **12/21/2024**

Table of Contents

HIPAA POLICY MANUAL ADDENDUM

Introduction

The Counseling Service's (TCS) intention for publishing this HIPAA Policy Manual is not to impose restrictions that are contrary to the company's established culture of openness, trust and integrity. TCS is committed to protecting employees, patients, partners and itself from illegal or damaging actions by individuals, either knowingly or unknowingly.

Effective HIPAA security is a team effort involving the participation and support of every TCS employee and affiliate that interacts with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

Any time that protected health information (PHI) is referenced in this policy, it is referencing the HIPAA Privacy Rule; when electronic protected health information (EPHI) is referenced in this policy, it is referencing the HIPAA Security Rule.

Scope

This HIPAA Policy Manual is applicable to the entire TCS organization and any outsourced service providers involved in TCS operational support.

Compliance and Enforcement

All TCS supervisors are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with TCS's Sanction Policy.

HIPAA-01: General HIPAA Compliance Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Introduction

TCS has adopted this General HIPAA Compliance Policy in order to recognize the requirement to comply with the Health Insurance Portability and Accountability Act ("HIPAA"), as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act of 2009 (Title XIII of division A and Title IV of division B of the American Recovery and Reinvestment Act "ARRA") and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013). We acknowledge that full compliance with the HIPAA Final Rule is required by or before September 23, 2013.

TCS hereby acknowledges our duty and responsibility to protect the privacy and security of Individually Identifiable Health Information ("IIHI") generally, and Protected Health Information ("PHI") as defined in the HIPAA Regulations, under the regulations implementing HIPAA, other federal and state laws protecting the confidentiality of personal information, and under principles of general and professional ethics. We also acknowledge our duty and responsibility to support and facilitate the timely and unimpeded flow of health information for lawful and appropriate purposes.

Scope of Policy

This policy governs General HIPAA Compliance for **TCS**. All personnel of **TCS** must comply with this policy as well as all the policies and procedures included within this HIPAA Policy Manual. Demonstrated competence in the requirements of this policy is an important part of the responsibilities of every member of the workforce.

Officers, agents, employees, Business Associates, contractors, affected vendors, temporary workers, and volunteers must read, understand, and comply with this policy in full and at all times.

Unless otherwise noted, any reference to IT Personnel or Network System Administrator shall relate to **TCS's** outsourced IT vendors, NetGain Technologies or Cyber Risk Management.

Assumptions

- **TCS** hereby recognizes its status as a Covered Entity under the definitions contained in the HIPAA Regulations.
- **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.
- Entities subject to HIPAA Rules are also subject to other federal statutes and regulations. For example, federal programs must comply with the statutes and regulations that govern them. Pursuant to their contracts, Medicare providers must comply with the requirements of the Privacy Act of 1974. Substance abuse treatment facilities are subject to the Substance Abuse

Confidentiality provisions of the Public Health Service Act, section 543 and its regulations. And, health care providers in schools, colleges, and universities may come within the purview of the Family Educational Rights and Privacy Act.

Policy Statement

- ❑ It is the Policy of **TCS** to become and to remain in full compliance with all the requirements of HIPAA.
- ❑ It is the Policy of **TCS** to fully document all HIPAA compliance-related activities and efforts, in accordance with our Documentation Policy.
- ❑ All HIPAA compliance-related documentation will be managed and maintained for a minimum of six years from the date of creation or last revision, whichever is later, in accordance with **TCS**'s Document Retention policy.

Procedures

In accordance with the amended HIPAA Final Rule (Effective Date: March 26, 2013), **TCS** commits to enacting, supporting, and maintaining the following procedures and activities, as a minimum, as required by HIPAA:

- ❑ **Risk Management Process** -- Implement and maintain an ongoing annual Risk Management Process that is consistent with the HIPAA Security Rule.
- ❑ **Privacy Policies and Procedures** -- **TCS** shall develop and implement written privacy policies and procedures that are consistent with the HIPAA Rules.
- ❑ **Security/Privacy Personnel** -- **TCS** shall designate a security official and a privacy official responsible for developing and implementing its privacy policies and procedures, and a contact person responsible for receiving complaints and providing individuals with information on **TCS**'s privacy practices.
- ❑ **Workforce Training and Management** -- Workforce members include employees, volunteers, trainees, and may also include other persons whose conduct is under the direct control of **TCS** (whether or not they are paid by **TCS**). **TCS** shall train all workforce members on its privacy policies and procedures, as necessary and appropriate for them to carry out their various functions.
- ❑ **Sanctions** -- **TCS** shall have and apply appropriate sanctions against workforce members who violate its privacy policies and procedures, and/or HIPAA's Privacy and Security Rules.
- ❑ **Mitigation** -- **TCS** shall mitigate, to the extent practicable, any harmful effect it learns was caused by use or disclosure of protected health information by its workforce or its business associates in violation of its privacy policies and procedures or the Privacy Rule.
- ❑ **Data Safeguards** -- **TCS** shall maintain reasonable and appropriate administrative, technical, and physical safeguards to prevent intentional or unintentional uses or disclosures of protected health information in violation of the Privacy Rule and its own policies, and to limit the incidental uses and disclosures pursuant to otherwise permitted or required uses or disclosures.
- ❑ **Complaints** -- **TCS** shall establish procedures for individuals to complain about its compliance with its privacy policies and procedures and the Privacy Rule. **TCS** shall explain those procedures in its privacy practices notice.
- ❑ **Retaliation and Waiver** -- **TCS** shall NOT retaliate against a person for exercising rights provided by HIPAA, for assisting in an investigation by HHS or another appropriate authority, or for opposing an act or practice that the person believes in good faith violates any HIPAA standard or requirement. **TCS** shall not require an individual to waive any right under the Privacy Rule as a condition for obtaining treatment, payment, and enrollment or benefits eligibility.

Compliance and Enforcement

All **TCS** personnel are responsible for enforcing this policy. Employees who violate this policy are subject to discipline up to and including termination in accordance with **TCS's** Sanction Policy.

HIPAA-02: HIPAA Policies and Procedures Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs the establishment and maintenance of policies and procedures 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, 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.

Policy Statement

- It is the Policy of **TCS** to create and implement appropriate policies and procedures as required by law and as suggested by good business practices and general business ethics. This shall include appropriate Security Policies and Procedures to address evolving security threats.
- All policies and procedures shall be updated and amended as needed or as required by law.
- All policies and procedures shall be distributed to, or made otherwise available to, the entire workforce.
- All policies and procedures shall be regularly maintained and secured, and copies shall be stored offsite with other important business records for safekeeping.
- All members of the workforce are required to read, understand, and comply with this and all other policies and procedures created and implemented by **TCS**.

Procedures

- **TCS** shall create or revise its own HIPAA policies and procedures, consistent with all applicable HIPAA Rules and Regulations as well as with applicable State laws and statutes.
- The Security and Privacy Officers shall assume control of the policies and procedures process. These individuals shall report to and shall execute the creation or revision process in a timely manner in compliance with current HIPAA guidelines.
- All Policies and Procedures will be reviewed at least once annually. Qualified counsel will be engaged as needed to guide or review the policies and procedures creation/revision process, to ensure they address all applicable HIPAA (and other) standards
- **TCS** shall internally publish its HIPAA policies and procedures to all workforce members, and shall provide appropriate training to all members of its workforce on the interpretation and implementation of its policies and procedures.

HIPAA-03: Documentation Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

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 Security Officer and/or 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. The HIPAA Privacy Officer's contact information will also be included in the agency's HIPAA Notice of Privacy Practices, which is contained in the client orientation packet.
- ❑ Each client and/or guardian signs and dates the consent for evaluation/treatment form which includes general HIPAA information as well as the company website to access more detailed HIPAA information, including the HIPAA Notice of Privacy Practices. The completed consent, 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. 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 maintained on the company's website and will be accessible to all employees. An annual all staff email notifying staff of the updated HIPAA Policies and Procedures will be sent out annually at the time of the completed review.
- ❑ 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 Security and 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 first creating an electronic, saved version of the documents.
- ❑ Data backup system will be implemented with appropriate backup job schedules and electronic data retention policies for ePHI to comply with this policy.

HIPAA-04: Investigations Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs HIPAA Investigations 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** recognizes that the U.S. Department of Health and Human Services ("HHS"), its Office for Civil Rights ("OCR") and other designees, as well as State Attorneys General, are all authorized and empowered to investigate Covered Entities and Business Associates in matters of HIPAA compliance and enforcement.
- **TCS** recognizes that timely and full cooperation with such investigative bodies is mandatory under HIPAA law; and that failure to cooperate with any HIPAA investigation is itself a violation of HIPAA Rules.

Policy Statement

- It is the Policy of **TCS** to fully comply with HIPAA law and with all HIPAA-related investigations conducted by HHS.
- It is the Policy of **TCS** to not impede or obstruct any HIPAA-related investigations conducted by HHS.
- It is the Policy of **TCS** to provide all documentation or assistance required by law in connection with any HIPAA-related investigations conducted by HHS.

Procedures

Workforce members who are designated to assist with HIPAA-related investigations conducted by HHS must adhere to the following procedures:

- Whenever a HHS investigation is discovered, the following contacts must be immediately notified:
  - Executive Director
  - Privacy Officer
  - Security Officer
  - Compliance Officer
  - Legal counsel
- Cooperate, but do not volunteer information or records that are not requested.
- Ask for the official government agency-issued identification of the investigators (Business cards are NOT official identification); write down their names, office addresses, telephone numbers, fax numbers and e-mail addresses. If investigators cannot produce acceptable I.D., call legal counsel immediately and defer the provision of any PHI until after you confer with counsel or until the investigators produce acceptable I.D. BE SURE that you've made appropriate requests for I.D. and that they've been unreasonably refused before you do.)
- Have at least one, if not two witnesses available to testify as to your requests and their responses.
- Permit the investigators to have access to protected health information ("PHI"), in accordance with our notice of privacy practices ("NPP"), and Federal and State law. Once investigators have verified their identities and have also verified their authority to access PHI, it is a violation of HIPAA to withhold PHI from them, if the PHI sought is the subject matter of the investigation, or reasonably related to the investigation. Again, ask investigators to verify that they are seeking

access to the information because it is directly related to their legitimate investigatory purposes; and document their responses in your own written records.

- ❑ Have a witness with you when you ask about their authority to access PHI, and the use that they will make of the PHI they are seeking access to, who can later testify as to what they told you. Two witnesses are even better. All witnesses should also prepare a written summary of the conduct and communications they observed as soon as possible after the incident; these summaries should be annotated with the time and date of the event, the time and date that the summaries were completed, and the witnesses signature.
- ❑ Send staff employees elsewhere, if possible, during this first investigation encounter. There is no requirement that we provide witnesses to be questioned during the initial phase of an investigation.
- ❑ Do NOT instruct employees to hide or conceal facts, or otherwise mislead investigators.
- ❑ Ask the investigators for documents related to the investigation. For example, request:
    - copies of any search warrants and/or entry and inspection orders
    - copies of any complaints
    - a list of patients they are interested in
    - a list of documents/items seized
- ❑ Do NOT expect that investigators will provide any of the above, except for the search warrant and a list of documents/items seized (if any).
- ❑ Do not leave the investigators alone, if possible. Assign someone to "assist" each investigator present.
- ❑ Do not offer food (coffee, if already prepared, and water, if already available, is ok). Don't do anything that could be construed as a "bribe" or a "kickback" to induce favorable treatment, such as offering to buy the investigators lunch.
- ❑ Tell investigators what you are required by law to tell them. Answer direct questions fully and to the best of your ability. Always defer to the advice of legal counsel if you are unsure of what or how much to say.

HIPAA-05: Breach Notification Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs Breach Notification 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 concerned with notifications to patients and consumers about breaches of individually identifiable health information, in accordance with the requirements at § 164.400 to § 164.414.
- ❑ Compliance with HIPAA's breach notification requirements is mandatory and failure to comply can bring severe sanctions and penalties.
- ❑ Timely notifications to consumers about breaches of individually identifiable health information can help reduce or prevent identity theft and fraud.
- ❑ Timely notifications to consumers about breaches of individually identifiable health information can help protect our business and reputation.
- ❑ Only breaches of "unsecured" (unencrypted or not destroyed) protected health information trigger HIPAA's breach notification requirements.

Definitions

As used within the HIPAA Final ("Omnibus") Rule, the following terms have the following meanings:

Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted **under subpart E of this part which compromises the security or privacy of the protected health information**.

- ❑ Breach excludes:

  a) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.

  b) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.

  c) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

- ❑ Except as provided in paragraph (1) of this definition, an acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a

low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

a) The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
b) The unauthorized person who used the protected health information or to whom the disclosure was made;
c) Whether the protected health information was actually acquired or viewed; and
d) The extent to which the risk to the protected health information has been mitigated.

Unsecured protected health information means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Pub. L. 111-5.

Policy Statement

- ❑ It is the Policy of **TCS** to provide timely notifications to affected (patients and/or) consumers about breaches of individually identifiable health information.
- ❑ **TCS** shall notify individuals when a reportable breach is discovered. A breach is treated as "discovered" by **TCS** the first day on which such breach is known or should reasonably have been known to any employee or agent of **TCS**, other than the person who committed the breach.
- ❑ Notification must occur without unreasonable delay upon discovery of the breach and consistent with the specified requirements of HHS, unless law enforcement requests a delay.

Procedures

- ❑ Breach Notices must include a brief description of what happened, a description of the types of PHI involved, steps the individual should take to protect themselves from potential harm, a brief description of the actions taken in response to the breach, and contact procedures for the individual to ask questions.
- ❑ For large breaches (affecting 500 or more individuals), first class mail shall be the default method of notification. **TCS** may use e-mail if requested by the individual, or substitute notice via our website or local print or broadcast media if we do not have current contact information.
- ❑ For small breaches (affecting less than 500 individuals), telephone shall be the default method of notification followed by timely documentation of the telephone conversation with the affected individual(s) and the affected individual(s) response. **TCS** may use e-mail if requested by the individual.
- ❑ **TCS** must notify major local media outlets of a breach affecting more than 500 individuals.
- ❑ Business Associates of **TCS** are required to immediately report all breaches, losses, or compromises of individually identifiable health information – whether secured or unsecured – to **TCS**'s designated Security Officer and/or Privacy Officer.
- ❑ Business Associate contracts, whether existing or new, shall have corresponding breach notification requirements included in them.
- ❑ Sanctions or re-training shall be applied to all workforce members who caused or created the conditions that allowed the breach to occur, according to **TCS**'s Sanction Policy.
- ❑ All breach-related activities and investigations shall be thoroughly and timely documented in accordance with **TCS**'s Documentation Policy.

HIPAA-06: Responsibilities of Privacy Officer Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs designation of a Privacy Official 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** recognizes that the designation of a Privacy Official is mandatory under the HIPAA Rules; and that the designation of a Privacy Official provides numerous benefits to **TCS.**

Policy Statement

- ❑ It is the Policy of **TCS** to designate and maintain at all times an active HIPAA Privacy-Official.
- ❑ The HIPAA Privacy-Official's general responsibilities are to work in conjunction with the TCS HIPAA Compliance Committee to:
  - Oversee all HIPAA-related compliance activities, including the development, implementation and maintenance of appropriate privacy and security-related policies and procedures.
  - Conduct various risk analyses, as needed or required.
  - Manage breach notification investigations, determinations, and responses, including breach notifications.
  - Develop or obtain appropriate privacy and security training for all workforce members, as appropriate.

Procedures

TCS's HIPAA Privacy Official, and their designee(s), shall be responsible for implementing, managing, and maintaining the following procedures:

- ❑ Ensure compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization's workforce, extended workforce, and for all business associates, in cooperation with the Executive Director, and legal counsel as applicable.
- ❑ Administer patient requests under HIPAA's Patient Rights.
- ❑ Administer the process for receiving, documenting, tracking, investigating, and taking action on all complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel.
- ❑ Cooperate with HHS and its Office for Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations.
- ❑ Develop specific policies and procedures mandated by HIPAA.
- ❑ Develop additional relevant policies, such as policies governing the inclusion of confidential data in emails, and access to confidential data by telecommuters.
- ❑ Draft and disseminate the Privacy Notice required by the Privacy Rule.
- ❑ Determine when consent or authorization is required for uses or disclosures of PHI, and draft forms as necessary.
- ❑ Ensure that all policies, procedures and notices are flexible enough to respond to new technologies and legal requirements, or, if they are not, work with the TCS HIPAA Compliance Committee to amend as necessary.
- ❑ Ensure that future initiatives are structured in such a way as to ensure patient privacy.
- ❑ Oversee employee training in the areas of information privacy.

- ❑ Deter retaliation against individuals who seek to enforce their own privacy rights or those of others.
- ❑ Oversee the evaluation of privacy implications of online, web-based applications.
- ❑ Oversee the monitoring of data collected by or posted on our website(s) for privacy concerns.

HIPAA-07: Assignment of Security Responsibility Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs the Assignment of Responsibility for health information data security 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 assignment of security responsibility, in accordance with the requirements at § 164.308(a)(2).
- ❑ The assignment of overall security responsibility is an important and integral part of our overall risk management process, and shall be conducted in accordance and coordination with our Risk Management Process Policy.

Policy Statement

- ❑ It is the Policy of **TCS** to fully document the assignment of overall security responsibility, and all related activities and efforts, according to our Documentation Policy and HIPAA requirements
- ❑ It is the Policy of **TCS** to assign overall responsibility for the security of individually identifiable health information, in electronic and other forms, to a person who is qualified and competent to assume such responsibility.
- ❑ The person with overall responsibility for the security of individually identifiable health information, in electronic and other forms, shall be the Security Officer, who shall report directly to the Executive Director. This person shall also work in conjunction with the TCS HIPAA Compliance Committee and other IT staff consultants to address the provisions of the HIPAA Security Rule.
- ❑ Appropriate training and support services shall be provided to the Security Officer to ensure he/she is kept abreast of evolving security issues and requirements.

Procedures

The HIPAA Security Officer, in consultation with the Executive Director, shall implement the following procedures, as appropriate, in accordance with **TCS**'s Risk Management policies:

- ❑ Periodically review the list of all individuals who have access to the Practice's confidential information, including PHI.
- ❑ Cooperate with the Office of Civil Rights, other legal entities, and organization officers in any compliance reviews or investigations.
- ❑ Work with appropriate technical personnel to protect the Practice's confidential information from unauthorized use or disclosure.
- ❑ Develop specific policies and procedures mandated by the Security Rule.
- ❑ Develop additional relevant policies, such as policies governing the inclusion of confidential data in emails, and access to confidential data by telecommuters.
- ❑ Review all contracts under which access to confidential data is given to outside entities, bring those contracts into compliance with HIPAA Rules to safeguard PHI, and ensure that the Practice's confidential data is adequately protected when such access is granted.

This review and oversight should include ensuring that current Business Associate Agreements are executed by appropriate vendors and maintained on file.

- ❑ Ensure that all policies, procedures and notices are flexible enough to respond to new technologies and legal requirements, or, if they are not, amend as necessary.
- ❑ Ensure that future Practice initiatives are structured in such a way to safeguard ePHI.
- ❑ Oversee periodic system audits and ensure remedial action is taken as necessary and authorized by the TCS HIPAA Compliance Committee.
- ❑ Oversee employee security awareness training and testing.
- ❑ Remain up-to-date and advise on new technologies to safeguard ePHI.
- ❑ Remain up-to-date on laws, rules and regulations regarding data privacy and update the Practice's policies and procedures as necessary.
- ❑ Monitor any data sharing initiatives for compliancy.

HIPAA-08: State Law Preemption Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs HIPAA Preemption and State Law 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 concerning state law preemptions of HIPAA regulations, in accordance with the requirements at § 160.201 to § 160.205.
- HIPAA generally preempts state laws regarding medical or health privacy. However, state laws that provide stronger protections for confidential health data, or that provide for better patient and consumer access to health data than HIPAA, will generally preempt HIPAA regulations.
- HIPAA Covered Entities and Business Associates must follow both HIPAA law and state law when possible. If there is a conflict between the two, a preemption analysis and determination must be made to assess which laws (HIPAA, State Laws, or both) must be followed.

Policy Statement

- It is the Policy of **TCS** to comply, whenever possible, with both state law in the state(s) where we operate, as well as HIPAA law and regulations.

Procedures

- **TCS**'s designated Privacy Official shall analyze HIPAA preemption issues, in cooperation with legal counsel, and make preemption determinations.
- **TCS**'s designated Privacy Official shall create, modify, or amend organization policies to accurately reflect preemption determinations and provide guidance to management on HIPAA and state law preemption issues.
- If off-the-shelf or custom preemption analyses are obtained from external sources, it is the responsibility of the **TCS**'s designated Privacy Official, in cooperation with legal counsel, to certify the validity and accuracy of such external preemption analyses before applying those analyses to **TCS** operations.
- **TCS**'s designated Privacy Official shall remain aware of legislative changes in the state(s) where we operate that could affect HIPAA preemption issues.

HIPAA-09: Training Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs HIPAA Privacy and Security Training 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 concerning the training of workforce members, in accordance with the requirements at § 164.530(b).
- Clear and complete HIPAA training, in combination with appropriate HIPAA awareness resources, can significantly reduce the likelihood of breaches of confidential health information and the likelihood of HIPAA violations.

Policy Statement

- It is the Policy of **TCS** to provide clear and complete HIPAA training to all members of the workforce, including officers, agents, employees, contractors, temporary workers, and volunteers.
- HIPAA training provided by **TCS** shall include relevant and appropriate aspects of both health data privacy and health data security, as it pertains to **TCS**'s operations and to the duties and responsibilities of specific individuals.

Procedures

- HIPAA training, at minimum, shall include the basics of HIPAA itself; the basics of HIPAA's privacy and security requirements and restrictions; and a review of relevant and appropriate internal Policies and Procedures related to HIPAA and HIPAA compliance.
- HIPAA training shall be provided to all new hires during the new employee orientation period, before new employees are exposed to or work with individually identifiable health information.
- HIPAA training shall be conducted periodically for all employees, but no less than every 12 months.
- All employees will be asked to sign a training verification checklist verifying that such training has been provided.
- Fostering ongoing, continuous HIPAA awareness shall be regarded as a separate type of workforce learning from regular HIPAA training. The designated HIPAA Privacy Official and/or Security Official shall be responsible for the development (or acquisition), and deployment of appropriate HIPAA awareness materials to maintain a high level of HIPAA awareness among the workforce. This awareness training should be updated periodically to reflect new cyber security threats.
- HIPAA training resources should aim to develop a general understanding of HIPAA and its requirements and restrictions. HIPAA awareness resources should aim to maintain a high level of HIPAA awareness, evolving security threats and a protective attitude toward confidential data on an ongoing, daily basis.

HIPAA-10: PHI Uses and Disclosures Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs the permitted uses and disclosures of Protected Health Information 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 concerning uses and disclosures of Protected Health Information, in accordance with the requirements at § 164.502 to § 164.514.
- ❑ **TCS** must implement policies and procedures to ensure that all uses and disclosures of PHI are made or denied in accordance with HIPAA law and regulations.
- ❑ For especially sensitive information, such as AIDS/HIV, alcohol and drug abuse prevention and treatment, and the like, patient consent to disclosure must be *informed*. That is, made with the patient's or consumer's knowledge of the risks and benefits of the disclosure.
- ❑ Any disclosure of confidential patient information carries with it the potential for an unauthorized redisclosure that breaches confidentiality.
- ❑ **TCS** incurs costs when releasing patient information (copying, postage, and so forth) and is permitted under HIPAA Regulations and under State law to charge a reasonable fee to offset those costs.

Policy Statement

- ❑ It is the Policy of **TCS** to conduct its operations in full compliance with HIPAA's Rules governing uses and disclosures of Protected Health Information.
- ❑ **TCS** will process requests for information from patient records in a timely, consistent manner as set forth in this policy.

Procedures

- ❑ The following priorities and time frames shall apply to requests for disclosures of PHI:
  - *Emergency requests involving immediate emergency care of patient:* immediate processing.
  - *Priority requests pertaining to current care of patient:* within one workday.
  - *Patient request for access to own record:* within (15) workdays.
  - *Subpoenas and depositions:* as required.
  - *All other requests:* within (15) workdays
- ❑ Courtesy Notifications to Practitioners – As a courtesy, records processing personnel shall notify the appropriate healthcare practitioner when any of the following occur:
  - Patient or his or her representative requests information from the medical record.
  - Patient or representative requests direct access to the complete medical record.
  - Patient or representative institutes legal action.
- ❑ Disclosure Monitoring-- Health Information Management personnel will review and update this log weekly to give proper priority to requests and to provide early intervention in problem situations. The log shall contain the following information:
  - Date department received the request.
  - Name of patient.

- Name and status (patient, parent, guardian) of person making request.
- Information released.
- Date released.
- Fee information, if applicable.

- ❑ Unless the request specifies release of the complete medical record, **TCS** shall release only selected portions of the record. **TCS** shall prepare an appropriate cover letter detailing the items included.
- ❑ Prohibition of Redisclosure -- Unless a law or regulation requires a more specific prohibition on re-disclosure (usually for AIDS/HIV, alcohol and drug abuse, and other particularly sensitive medical information), each disclosure outside the facility shall contain the following notice or a similar notice containing the prohibition of further disclosure (such as the *Notice of Prohibition on Disclosure* included on the bottom of the fax cover sheet).
  - *The attached medical information pertaining to [Name of patient] is confidential and legally privileged. **TCS** has provided it to [Name of recipient] as authorized by the patient. The recipient may not further disclose the information without the express consent of the patient or as authorized by law.*
- ❑ Retention of Disclosure Requests -- The designated Security Officer and/or Privacy Officer will retain the original request, the authorization for release of information, and a copy of the cover letter and any other relevant documents pertaining to the request in the appropriate secure electronic filing system for the appropriate record retention period.
- ❑ Disclosure Quality Control -- The Executive Director and/or the designated Security Officer and/or Privacy Official shall conduct a routine audit of the release of information at least annually, paying particular attention to the following:
  - Validity of authorizations.
  - Appropriateness of information abstracted in response to the request.
  - Retention of authorization, request, and transmitting cover letter.
  - Procedures for telephone, electronic, and in-person requests.
  - Compliance with designated priorities and time frames.
  - Proper processing of fees.
  - Maintenance of confidentiality.
- ❑ In-service Training on Disclosures -- The Executive Director in conjunction with the Security Officer and/or Privacy Official shall give periodic in-service training and/or ongoing training through the use of all staff email reminders to all employees involved in the release of information.
- ❑ Annual Policy Review - The Security and/or Privacy Official shall review this policy and associated procedures with risk management and legal counsel at least annually.

- Capacity to Authorize – TCS requires a written, signed, current, valid authorization to release medical information as follows:

Patient Category	Required Signature
Adult Patient	The patient or a duly authorized representative, such as court-appointed guardian or attorney. Proof of authorized representation required (such as notarized power of attorney).
Deceased Patient	Next of kin as stated on admission face sheet (state relationship on authorization) or executor/ administrator of estate.
Unemancipated Minor	Parent, next of kin, or legally appointed guardian or attorney (proof of relationship required).
Emancipated Minor	Same as adult patients above.
Psychiatric, drug, alcohol program patients/clients	Same as adult patients above, but check for special requirements.
AIDS/HIV or other sexually transmitted disease patients	Same as adult patients above, check for special requirements.

- Authorization Forms -- The Executive Director and/or the designated Security Official and/or Privacy Official shall develop and use an approved authorization form. All personnel will use this form whenever possible. All personnel shall, however, honor letters and other forms, provided they include all the required information.
- Revocation of Authorization -- A patient may revoke an authorization by providing a written statement to us. The revocation shall become effective when the facility receives it, but shall not apply to disclosures already made.
- Refusal to Honor Authorization – The Executive Director and/or the designated Security and/or Privacy Official, or others authorized to release information, will not honor a patient authorization when they have a reasonable doubt or question as to the following information:
    - Identity of the person presenting the authorization.
    - Status of the individual as the duly appointed representative of a minor, deceased, or incompetent person.
    - Legal age or status as an emancipated minor.
    - Patient capacity to understand the meaning of the authorization.
    - Authenticity of the patient(s) signature.
    - Current validity of the authorization.
    - In such situations, the employee shall refer the matter to the Executive Director in conjunction with the Security and/or Privacy Officer for review and decision.
- Electronic Records -- The above requirements apply equally to electronic records. No employee shall release electronic records without complying with this policy.

Note: See Addendum for Person and Identity Verification and PHI Disclosures Tables

HIPAA-11: Patient Rights Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs the provision and management of Patient Rights 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, in accordance with the requirements pertaining to the rights of patients at § 164.520, to § 164.528, as amended by HITECH Act of 2009 (ARRA Title XIII), and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013).
- ❑ Patient information related to patient rights includes only that information contained in each patient's Designated Record Set ("DRS"), defined in the HIPAA regulations at § 164.501 as:
  - A group of records maintained by or for a covered entity that is:
    - The medical records and billing records about individuals maintained by or for a covered health care provider;
    - The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
    - Used, in whole or in part, by or for the covered entity to make decisions about individuals.
  - The term "record" means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.
- ❑ The provision of patient rights in a timely and positive manner can enhance the quality of care we provide to patients, by providing certain rights and controls to patients over their individually identifiable health information.

Policy Statement

- ❑ It is the Policy of **TCS** to provide all the patient rights to our patients that are called for in the HIPAA regulations. Patient Rights that we provide and support include:
  - The Right to receive a copy of our "Notice of Privacy Practices", which details how individually identifiable health information may be used or disclosed by this organization.
  - The Right to review or obtain a copy of medical records about that patient, or about the patient's minor children.
  - The Right to request restrictions on the use or disclosure of the patient's medical records.
  - The Right to receive individually identifiable health information at an alternate address or through alternate delivery means, such as by fax or courier.
  - The Right to request amendments to medical records, with certain limitations.
  - The Right to an accounting of certain disclosures of individually identifiable health information.
  - The Right to file a privacy complaint directly with us, or with the federal government.
- ❑ No retaliation of any kind is permitted against any person, patient, or workforce member for exercising any Right guaranteed by HIPAA.

Procedures

- ❑ A document outlining the Patient Rights will be included in the orientation packet/The Client Handbook and access to this information made known at the time of service initiation.
- ❑ The agency's HIPAA Notice of Privacy Practices and/or a reference to the availability of the document on the company website and upon request will be included in the orientation packet given to all clients at the time services are initiated.
- ❑ The orientation packet will include contact information for the agency's Patient Rights Officer and the agency's Privacy Officer.

HIPAA-12: Privacy Complaints Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs the privacy complaints process 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 privacy complaints in accordance with the requirements at § 164.530(a) and § 164.530(d), as amended by the HITECH Act of 2009 (ARRA Title XIII), and the HIPAA Omnibus Final Rule (Effective Date: March 26, 2013).
- ❑ HIPAA regulations, at § 164.530(g), prohibit intimidating or retaliatory acts against any person or patient who files a privacy complaint or exercises any Right guaranteed under HIPAA.

Policy Statement

- ❑ It is the Policy of **TCS** to respond in a timely and positive manner to all complaints submitted by any persons or parties, including patients, workforce members, and any other person or party.
- ❑ Responsibility for the acceptance of, management of, and responses to complaints shall reside with the designated HIPAA Privacy Officer, in consultation with the agency's Executive Director.

Procedures

- ❑ All complaints must be submitted in written form, dated and signed by the complainant.
- ❑ **TCS** shall investigate and respond to all complaints with a written response within 30 days of the time each complaint is submitted in writing. If more time is required to investigate and resolve a specific complaint, the complainant shall be notified in writing within 30 days of the time each complaint is submitted in writing, that additional time is required to investigate and resolve the complaint. In no case shall more than 60 days elapse between the time a complaint is submitted in writing and the resolution of the complaint.
- ❑ The designated HIPAA Privacy Officer shall investigate each and every complaint in a fair, impartial, and unbiased manner. All parties named in the complaint, or who participated in events leading to the complaint, shall be interviewed in a non-threatening and non-coercive manner. In the event that the HIPAA Privacy Officer is the subject of the formal complaint filed, the Security Officer will assume responsibility of the investigation and handling of the complaint.
- ❑ The final resolution or disposition of each complaint shall be documented in accordance with **TCS**'s Documentation Policy, and shall be retained in accordance with **TCS**'s Documentation Retention Policy.
- ❑ The final resolution or disposition of each complaint shall be documented and a summary of the findings shall be provided to the complainant within 30 days of the time each complaint is submitted in writing, unless the additional 30-days of response time is invoked, as above.
- ❑ In addition to providing complainants with a written response to their complaint, complaints that are found to have merit will be resolved with some remediation that is appropriate to the severity of the situation. Such remediation may include, but are not limited to:
  - A written apology to the complainant from our organization.
  - Credit-monitoring service for the complainant for a period of one or two years, paid for by our organization, when the complaint involves a breach of unsecured individually identifiable health information that has been compromised or put at risk by our actions.
  - Financial compensation, if determined to be appropriate by legal counsel and senior management.
  - Sanctions against workforce members, as appropriate to the circumstances.

- Other unspecified remediation(s), as determined by legal counsel and senior management.

- ❑ For complaints submitted to the federal government, it is the Policy of **TCS** to cooperate fully and openly with federal authorities as they conduct their investigation, as specified in **TCS's** HHS Investigations Policy.
- ❑ No officer, agent, employee, contractor, temporary worker, or volunteer of **TCS** shall obstruct or impede any investigation in any way, whether internal or federal.

HIPAA-13: Risk Management Process Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs the establishment and maintenance of a Risk Management Process for **TCS**. This Risk Management Process Policy shall encompass a comprehensive range of activities including an incorporated Risk Analysis and Annual Security Risk Management Plan.

Two key principal components involved in the risk management process are Risk Analysis and Risk Management Process:

- **Risk Analysis:** 164.308(a)(1)(ii)(A) R - Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic Protected Health Information (ePHI) held by the covered entity.
- **Risk Management:** 164.308(a)(1)(ii)(B) R - Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with *164.306(a).

Assumptions

- **TCS** must comply with HIPAA and the HIPAA implementing regulations pertaining to the establishment and management of an appropriate risk management process, in accordance with the requirements at § 164.302 to § 164.318.
- The establishment and maintenance of an appropriate risk management process will generally reduce our privacy and security risk, can reduce the likelihood of creating HIPAA violations, whether inadvertent or intentional.

Policy Statement

- It is the Policy of **TCS** to establish, implement, and maintain an appropriate Risk Management Process. This Policy shall include a periodic Risk Analysis and annual Risk Management Plan as integral components in the Risk Management Process.
- **Risk Management Process** - Our risk management process shall strive to identify, analyze, prioritize, and minimize identified risks to information privacy, security, integrity, and availability. The nature and severity of various risk and risk elements shall be identified and quantified, with the goal of reducing risk as much as is practicable. The risk management process shall be ongoing, and shall be updated, analyzed, and improved on a continuous basis.
- **Risk Analysis** – A Risk Analysis is an integral part of the organization's overall Risk Management Process Policy and process and shall be conducted periodically in order to assess potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic Protected Health Information ("ePHI") that the organization has been entrusted with.
- **Risk Management Implementation** – Upon completion of each Risk Analysis conducted, an associated Risk Management implementation plan shall be developed. This plan will include a list of any HIPAA security gaps identified with associated recommendations to remediate risks. It shall be the responsibility of the Executive Director working with the HIPAA Officials to prioritize issues be remediated within a specific timetable. Any HIPAA compliance gaps or vulnerabilities identified that are not approved for remediation shall be documented in the plan with explanation for cause and acknowledgement of residual risk assumed on behalf of the organization.
- The results of the risk management process shall be input into management's decision-making processes, in order to help reduce our overall risk and to comply with HIPAA and other applicable laws and regulations.

- ❑ The risk management process shall be under the direct control and supervision of the Executive Director, and shall involve legal counsel, information technology, and any other parties or persons deemed to be appropriate to the process.
- ❑ Responsibility for conducting periodic risk analyses shall be with the designated HIPAA Security Officer, in consultation with the agency's Executive Director, IT consultants, and the HIPAA committee, who shall establish a plan and procedures for the conduct of such analyses.

Procedures

- ❑ Feedback will be solicited on a periodic and as needed basis from all employees surrounding perceived risks to information privacy, security, integrity, and availability.
- ❑ Any identified risks will be investigated and mitigated accordingly.
- ❑ Privacy-related risks will also be considered during the updating of the agency's Risk-Management Plan, which occurs annually.
- ❑ Risk analyses and assessments shall be conducted annually and as deemed necessary by the HIPAA Committee.
- ❑ The results of risk analyses and assessments shall become an integral part of management's decision-making process, and shall guide decisions related to the protection of Protected Health Information.
- ❑ All such risk analyses and assessments shall be documented in accordance with this organization's Documentation Policy and HIPAA Regulations.
- ❑ The specific mitigation measures identified will be implemented in the most expeditious manner possible to minimize the risk of additional or increased vulnerability in the future.
- ❑ Follow-up efforts will be employed to ensure mitigation measures had the desired effect.

HIPAA-14: Sanction Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs Workforce Sanctions and disciplinary actions 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 workforce-member sanctions, in accordance with the requirements at § 164.308(a)(1).
- Appropriate, fair and consistent sanctions have a deterrent influence on workforce transgressions; can help prevent breaches of individually identifiable health information and Protected Health Information, and can help prevent, or reduce the severity, of HIPAA violations.

Policy Statement

- It is the Policy of **TCS** to establish and implement appropriate, fair and consistent sanctions for workforce members who fail to follow established policies and procedures relative to HIPAA compliance, or who commit various offenses.
- Sanctions applied shall be appropriate to the nature and severity of the error or offense, and shall consist of an escalating scale of sanctions, with less severe sanctions applied to less severe errors and offenses, and more severe sanctions applied to more severe errors and offenses.
- It is the Policy of **TCS** to fully document all HIPAA-related workforce sanctions and their dispositions, according to our Documentation Policy and HIPAA requirements.

Procedures

- All employees will be trained on HIPAA related policies and procedures at the time of New Hire Orientation.
- All employees will be trained upon hire and annually thereafter on the agency's Corporate Compliance Programs, which affirms the agency's commitment to legal and ethical behavior in all aspects of its operations—including maintenance of client records in accordance with HIPAA.
- All employees are asked to sign off on a Training Verification form confirming that such training has been provided.
- Any employee in violation of a policy or engaged in violation of HIPAA will be reprimanded in a manner considered reasonable and appropriate in relation to the severity of the offense, as determined by the agency's Executive Director.

HIPAA-15: Information Systems Activity Review Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs Information Systems Activity Reviews 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 information systems activity review, in accordance with the requirements at § 164.308(a)(1).

Policy Statement

- It is the Policy of **TCS** to regularly review various indicators and records of information system activity, including, but not limited to: audit logs; access reports; and security incident reports.
- The goal of this Information Systems Activity Review Policy is to prevent, detect, contain, and correct security violations and threats to individually identifiable health information, whether in electronic or any other forms.
- It is the Policy of **TCS** to fully document all information system activity review activities and efforts.
- This Information Systems Activity Review Policy shall be implemented and executed in accordance with our risk management policies and procedures.

Procedures

- The Network Systems Administrator shall review Security Event Logs, System Access Rights and Auditable Access Logs no less than monthly.
- The Network System Administrator shall log any pertinent findings and submit a monthly report to the HIPAA Compliance Committee that provides a summary recap of any findings and status of any remediation.
- Monthly Log Reviews and Quarterly Vulnerability Scans will be conducted by the Network Administrator. Printed reports generated will be stored electronically and will be included as deemed necessary for organization and review in a binder in TCS's administrative office.

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

Effective Date:	12-01-2015	Last Revised:	12-21-2023

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.

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.
- Performance 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.
- An active check of Active Directory to ensure all users are still employed will occur at least quarterly, and more frequently, if appropriate.

HIPAA-17: Workforce Clearance Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs Workforce Clearance and Screening (pre-employment and post-employment) 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 workforce clearance, in accordance with the requirements at § 164.308(a)(3).
- Providing for appropriate workforce clearance can help reduce the likelihood of data breaches and HIPAA violations.

Policy Statement

- It is the Policy of **TCS** to provide the appropriate level of access to individually identifiable health information to all members of the workforce.
- The level of access to individually identifiable health information for workforce members shall be based upon the nature of each workforce member's job and its associated duties and responsibilities. Workforce members shall have access to all of the individually identifiable health information that they need to do their jobs, but no more access than that.
- No member of the workforce shall have access to a higher level of individually identifiable health information than the level for which they have been cleared.
- The Executive Director, in consultation with HIPAA Officers and appropriate IT personnel, shall develop specific procedures to ensure that the intent of this policy is executed in fact.
- Workforce clearance shall specifically incorporate various levels of background screening to ensure that persons with criminal records or those who appear on government exclusion lists do not have inappropriate access to individually identifiable health information.
- The Executive Director shall coordinate background screening requirements with Human Resources and legal counsel to ensure that appropriate background screening requirements are established and met, which can include pre-employment and post-employment screening.
- It is the Policy of **TCS** to fully document all workforce clearance-related activities and efforts.

Procedures

- All new employees are subject to fingerprinting and a criminal background check at the time of New Hire Orientation. Such information is retained in the employee's personnel file.
- Only active employees will have valid usernames and passwords granting access to PHI.
- **TCS** employs a role-based accessed system, meaning that all individual employee 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, supervisory oversight activities, peer review or other quality improvement efforts, and coordination of billing activities.
- 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.

HIPAA-18: Access Termination Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs the termination of individual access to individually identifiable health information and Protected Health Information 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 termination of workforce member access to individually identifiable health information and Protected Health Information, in accordance with the requirements at § 164.308(a)(3).
- Prompt and appropriate termination of workforce member access to individually identifiable health information and Protected Health Information can greatly reduce the likelihood of data breaches and HIPAA violations.

Policy Statement

- It is the Policy of **TCS** to terminate any workforce member's access to individually identifiable health information and Protected Health Information when their employment relationship with our organization ends, or when the workforce member has been sanctioned for serious offenses or violations of policy, in accordance with our Sanction Policy.
- Termination of workforce member's access to individually identifiable health information and Protected Health Information must be effected as soon as feasible upon the occurrence of a triggering event, such as termination of employment or a positive finding of a serious policy violation or HIPAA offense.
- In no case shall the termination of access to individually identifiable health information and Protected Health Information be delayed more than 24 hours from the moment of such a triggering event. In cases of involuntary termination, access will be terminated within one working day of the return of all **TCS** equipment. In cases of voluntary termination, access to individually identifiable health information and Protected Health Information will be terminated within 24 hours of completion of work-related tasks.
- It is the Policy of **TCS** to fully document all access termination-related activities, in accordance with our Documentation Policy.

Procedures

- A termination checklist will be developed and maintained for use by the Executive Director and supporting staff (HR, IT, Facilities Mgt, etc.) in order to help ensure timely workflow and compliance with this Access Termination Policy. Items to be included in this checklist included but not limited to:
  a) Upon termination of any workforce member's employment, usernames and passwords to the network as well as all applications containing ePHI will be disabled within the time period defined in above termination policy.
  b) Company-owned smart phones (if assigned) will be turned in immediately upon termination of one's employment. Staff member personal cell phones that had been approved for use in TCS email will be verified as clean based on existing BYOD policy.
  c) Workplace keys will be turned in immediately upon termination of one's employment.
  d) Any TCS Identification badge will be turned in immediately upon termination of employment.
  e) Company-owned laptops (if assigned) will be turned in immediately upon termination of one's employment and completion of remaining clinical documentation.
  f) All clinical documentation will be completed and validated prior to termination of one's employment.

HIPAA-19: Security Reminders Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs the creation and implementation of Security Reminders 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 security reminders, in accordance with the requirements at § 164.308(a)(5).
- The frequent use of appropriate security reminders and other information security awareness resources can reduce the likelihood of data breaches and HIPAA violations.

Policy Statement

- It is the Policy of **TCS** to develop or acquire and to use appropriate information security reminders, or other information security awareness resources, on a regular basis.
- The HIPAA Security Officer shall assume responsibility for developing or acquiring such reminders and resources, and for implementing a plan and program ensuring their frequent use.
- It is the Policy of **TCS** to fully document all information security reminder-related activities and efforts, according to our Documentation Policy.

Procedures

- HIPAA compliance reminders will be issued at Quarterly Meetings.
- HIPAA Privacy and Security Reminders will also be distributed via periodic internal emails.

HIPAA-20: Endpoint Computer Security Policy

Effective Date:	7/1/2018	Last Revised:	12-21-2023

Scope of Policy

This policy governs Endpoint security for all TCS Servers and Desktop/Laptop Computers for **TCS**. All personnel of **TCS** must comply with this policy. Demonstrated competence and compliance with 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 protection from so-called malware, in accordance with the requirements at § 164.308(a)(5).
- The use of appropriate techniques, technologies, and methods to update critical security patches and protect information systems from malicious software ("malware") is a proven approach to reducing the likelihood of data breaches, system malfunctions, and HIPAA violations.

Policy Statement

Effective compliance with HIPAA Security Rule requires that TCS implement and maintain an appropriate endpoint security policy and procedures. The purpose of this policy is to ensure that all workforce members understand the importance of maintaining updated security patches and endpoint security software definitions on their assigned desktop/laptop computers, as well as all Servers.

- Workstations and other computer systems are provided to employees for the purpose of performing their job functions. Employees shall be responsible for using workstations appropriately in conformance with this Policy. *This shall include following TCS's standard policy and procedures to maintain effective desktop security.*
- An effective security patch management process will be maintained to ensure that security patches are applied to all workstations, servers and portable devices, where feasible. Leading third party applications (i.e., browsers, Adobe, Java, etc.) will also be included in the TCS patch management process as well to ensure that all relevant security patches and updates are promptly applied based on the severity of the vulnerability corrected. Any other applications should be manually updated with any new security patches released.
- An approved endpoint security (anti-virus / anti-malware) software that protects against malicious software will be deployed and maintained on all workstations, servers and portable devices. The Endpoint Security software must be current and up to date with new virus / malware definitions. Employees must use and keep active current versions of approved anti-virus / anti-malware software scanning tools to detect and remove malicious software from workstations and files. Employees must not disable these tools unless specifically directed by computer support personnel to do so in order to resolve a particular problem.
- Security Awareness Training shall include information on emerging cybersecurity concerns, and associated email threats.
- Workforce members shall comply with all TCS training regarding security best practices at all times, including accessing any public Wi-Fi connections, and being aware of man-in-the-middle threats.
- Responsibility for enforcement of this policy shall reside with the Executive Director, in consultation with the appropriate IT personnel, who shall ensure that the most effective and appropriate techniques, technologies, and methods are continuously used to protect our information systems, and the individually identifiable health information they contain, from security threats.
- It is the Policy of **TCS** to fully document all endpoint protection-related activities and efforts, in accordance with our Documentation Policy.

Procedures:

- ❑ Endpoint security software will be installed, monitored, and maintained by designated IT personnel, who will be responsible for reporting status of efforts and issues to Security Officer and/or Executive Director on a regular basis.
- ❑ A management agent will be installed on all workstations in order to manage the deployment of approved security patches as well as monitoring the status of endpoint security updates.
- ❑ Both of these processes required staff computers to be left on overnight while connected to the internet. If there is not time for updates during normal work hours, then the computer should be left one or more nights a week pursuant to instructions provided by the Executive Director or the IT Staff. A reminder to connect the computer to the internet and to leave the computer on for several hours or overnight will be emailed to staff on a reoccurring basis.
- ❑ Any remote access to the TCS network shall require an approved VPN client.

HIPAA-21: Log-In Monitoring Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs Log-In Monitoring 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 log-in monitoring, in accordance with the requirements at § 164.308(a)(5).
- Regular monitoring of log-ins and log-in attempts is a proven approach to controlling access to sensitive information systems and data, and to detecting inappropriate information systems activity.
- The monitoring of successful and unsuccessful Log-In attempts is also a well established method of detecting malicious intrusions, and intrusion attempts, into information systems by unauthorized persons.

Policy Statement

- It is the Policy of **TCS** to establish a program of regular monitoring and review of log-ins and log-in attempts.
- IT Personnel, in consultation with the Executive Director and HIPAA Compliance team, shall assume responsibility for ensuring appropriate monitoring and analysis of log-in attempts occurs that such activities are executed on a continuous and ongoing basis.
- Discrepancies and potentially inappropriate or illegal activities shall immediately be brought to the attention of senior management, legal counsel, and/or Human Resources, as appropriate.
- It is the Policy of **TCS** to fully document all log-in monitoring-related activities and efforts, in accordance with our Documentation Policy.

Procedures

- TCS shall develop, implement, and regularly review a formal, documented process for monitoring login attempts and reporting discrepancies.
- Access to all information systems must be via a secure login process. At a minimum, the process should:
  - Validate login information only when all data has been input. If an error occurs, the system must not indicate which part of the data is correct or incorrect.
  - Limit the number of unsuccessful login attempts allowed.
  - Include the potential use of multiple challenge questions if a password is forgotten to aid in password reset.
- Information systems' login process should include the ability to:
  - Record unsuccessful login attempts.
  - After a specific number of failed login attempts, enforce a time delay before further login attempts are allowed or reject any further attempts without authorization from an appropriate workforce member.
  - Limit the maximum time allowed for the login process.

HIPAA-22: Password Management Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs information systems Password Management 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 password management, in accordance with the requirements at § 164.308(a)(5).
- The creation and management of strong passwords is one of the simplest and most effective methods of protecting access to electronic systems containing, transmitting, receiving, or using individually identifiable health information.
- The use of an approved Password Manager is also an effective method for generating and securing complex passwords for multiple systems.

Policy Statement

- It is the Policy of **TCS** to require the use of strong and complex passwords by all workforce members who access, use, or maintain systems that contain, transmit, receive, or use individually identifiable health information.
- The responsibility for implementing this policy and any attendant procedures is hereby assigned to the Executive Director, who shall develop and implement this policy in coordination with the most senior information technology personnel.

Procedures

- All passwords used to access systems containing, transmitting, receiving, or using individually identifiable health information shall be a minimum of ten (10) characters in length, and should include non-alphanumeric characters or symbols in them.
- Passwords should be changed by users at least once every twenty-four (24) months, pending unforeseen/emergency situations that may interfere with ability to update on this schedule.
- In the event of an information system compromise, as determined by the designated HIPAA Official or HIPAA Officer, some or all workforce-member passwords may need to be changed. This determination shall be made by the most senior IT personnel in consultation with the Executive Director.
- Under no circumstances shall passwords be written down and kept at or near computers and workstations where they may be found by others. Passwords may, however, be written down and stored in a workforce member's wallet or purse, if the password is thus afforded protection equal to the protection afforded to workforce members' cash, credit cards, and other critical documents.
- Any workforce member who loses, misplaces, forgets, or experiences any compromise of their password shall immediately notify HIPAA Security Officer, or, if they are unavailable, shall notify the Executive Director. Such notification of password compromise must be made *immediately* to the contact(s) indicated herein, but in no case shall such notification be delayed more than one (1) hour.
- Proper password management shall be emphasized in HIPAA training programs, in security reminders, and in any HIPAA security awareness resources used by this organization.

HIPAA-23: Security Incident Procedures

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs responses to Security Incidents involving the breach or compromise of Protected Health Information 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 security incident procedures, in accordance with the requirements at § 164.308(a)(6) and at § 164.400 to 164.414.
- Appropriate responses to security incidents may include, but are not limited to:
  - Rapid identification and classification of the severity of security incidents.
  - Determination of the actual risk to individually identifiable health information, and the subject(s) thereof.
  - Repairing, patching, or otherwise correcting the condition or error that created the security incident.
  - Retrieving or limiting the dissemination of individually identifiable health information, if possible.
  - Determining if the security incident rises to the level of a reportable breach under the HIPAA regulations.
  - Making a lawful and appropriate report of a breach, if required, to the appropriate parties. Appropriate parties to whom breaches must be reported, as defined by HIPAA regulations, may include, but are not limited to: *Patients, Consumers, Regulatory Authorities, including HHS and/or the Federal Trade Commission Law Enforcement and the local media, if necessary and required by law.*
  - Mitigating any harmful effects of the security incident.
  - Fully documenting security incidents, along with their causes and our responses.
  - Expanding our knowledge of security incident prevention, through research, analyses of security incidents, and improved training and awareness programs for workforce members.
- Compliance with HIPAA's data protection requirements is mandatory and failure to comply can bring severe sanctions and penalties.

Policy Statement

- It is the Policy of **TCS** to rapidly identify and appropriately respond to all security incidents, regardless of their severity.
- Responsibility for responding to and managing security incidents shall reside with HIPAA Privacy & Security Officers in consultation with the Executive Director.
- It is the Policy of **TCS** to fully document all security incidents and our responses thereto, in accordance with our Documentation Policy and HIPAA requirements.

Procedures

- All employees will be trained on HIPAA related policies, including the requirement to report anything determined to pose a risk, regardless of the severity, to the security of PHI. Such training will occur at New Hire Orientation and annually thereafter.
- When a security incident is reported, the details of the incident will be fully documented, as well as any follow-up efforts or notifications made as deemed appropriated and necessary by the HIPAA Privacy and Security Officers in consultation with the Executive Director.

HIPAA-24 Data Backup and Storage Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs Data Backups and Storage 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 data backups and storage, in accordance with the requirements at § 164.308(a)(7) and § 164.310(d)(1-2).
- The ability to create and maintain retrievable, exact copies of individually identifiable health information generally, and Electronic Protected Health Information specifically, is a critical element of our business operations and our ability to respond to unexpected negative events.
- The storage of data backups in a separate location, removed from our normal business operations ("offsite") is an essential element of any successful data backup plan.
- Timely access to health information is crucial to providing high quality health care, and to our business operations.
- Physicians, healthcare providers and others must have immediate, around-the-clock access to patient information.
- No existing media are absolutely guaranteed to provide long-term storage without loss or corruption of data.
- A number of risks to health information exist, such as power spikes or outages, fire, flood, or other natural disaster, viruses, hackers, and improper acts by employees and others.

Policy Statement

- It is the Policy of **TCS** to create and maintain complete, retrievable, exact backups of all individually identifiable health information generally, and Electronic Protected Health Information specifically, held, processed, or stored in the course of business operations, in full compliance with all the requirements of HIPAA.
- This policy includes creating retrievable, exact copies of electronic protected health information, when needed, before any movement or maintenance of data processing equipment that could result in the loss or compromise of electronic protected health information.
- All data backups shall be created and maintained in such manner as to ensure the maximum degree of data integrity, availability, and confidentiality are maintained at all times. This shall include an understanding of the organization's **Recovery Time Objectives** (amount of time to recover data) and **Recovery Point Objective** (amount of data that would be lost)
- Data backup jobs and retention policies will be implemented in accordance with the Document/Data Retention Policy and reviewed periodically to ensure compliance.

Procedures

- **TCS** will back up all such data automatically using an appropriate commercial backup solution based on backup policies which support established Recovery Point Objectives and data retention schedule.
- The Network System Administrator is responsible for performing daily backups on **TCS**'s network, including shared drives containing application data, patient information, financial data, and crucial system information

- ❑ If a Disk-to-Disk Backup solution is utilized, such backup data will be securely replicated to a secured off-site location and maintained in an encrypted status by a responsible organization who shall execute a HIPAA Business Associate Agreement**.** *If a local copy of backup data is maintained on site it will also be encrypted.* If a backup solution using removal backup media is utilized, such media shall be encrypted and stored in a secured off-site location. The media storage vault shall meet fire and disaster standards for such backup media and will be kept locked at all times. Only the organization's authorized HIPAA officers, the network system administrator, and the Executive Director's designees shall have access to the media storage vault. In the event that the off-site secured media vault is not available or properly functioning, the, network system administrator, or Executive Director's designees will remove onsite backup media to a secured offsite location until the media vault becomes available.
- ❑ The network system administrator or other designated individuals shall validate the daily backup jobs, will generate daily reports and maintain such reports for a minimum of 30 days.
- ❑ Any errors will be acted upon immediately. Responsible personnel will use contracted technical support as needed to resolve problems and ensure the validity of backup data.
- ❑ The Network System Administrator is responsible for periodically testing the validity of backup data and the ability to restore data in the event of a computer system problem, failure, or other disaster at least quarterly and more often if necessary to ensure data restores are sufficient to maintain data integrity, availability, and confidentiality.
- ❑ Successful restore functions must be logged in the network log. Any problems identified during the restore function must be acted on immediately and no later than the same business day that they occur. Responsible personnel will use contract technical support as needed to resolve problems and ensure the validity of backup data.
- ❑ All personnel who detect or suspect a data backup problem should immediately report the same to the Network System Administrator. Such personnel should follow up immediate notification with a written memorandum that includes the following information:
    - Narrative of the data backup problem.
    - How long the problem has existed.
    - Suggested solutions.

HIPAA-25: Disaster Recovery Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs contingency Disaster Recovery Planning 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 disaster recovery, in accordance with the requirements at § 164.308(a)(7).
- ❑ HIPAA requires **TCS** to establish and implement processes and procedures for responding effectively to emergencies or other occurrences (fire, vandalism, system failure, and natural disaster, etc.) that damage systems containing electronic protected health information.
- ❑ A disaster may occur at any time, not necessarily during work hours.
- ❑ **TCS** must remain operational with as little disruption of business operations and patient care as possible.
- ❑ Continuity of patient care requires uninterrupted access to patient information.
- ❑ In a dangerous emergency, evacuating personnel has priority over preserving information assets.
- ❑ The following conditions can destroy or disrupt **TCS**'s information systems:
  - Power interruption.
  - Fire.
  - Water.
  - Weather and other natural phenomena, such as earthquakes.
  - Sabotage and vandalism.
  - Terrorism.

Policy Statement

It is the policy of **TCS** to establish and implement processes and procedures to create and maintain retrievable exact copies of electronic protected health information in order to be able to reinstall and recover in the case of any data corruption or other disaster within sufficient time to maintain business operations and patient care levels.

Procedures

Preventive Measures:

- ❑ The Executive Director and or their designee(s) shall ensure that the following preventive measures, as applicable, are implemented and documented:
  - Back up computer systems and data files according to our Data Backup Policy.
  - Maintain secure backup data in the off-site media vault, according to our Data Backup Policy.
  - Maintain and replace any portable media according to our Data Backup Policy.
  - Test integrity of backup system according to our Data Backup Policy.
  - Disaster Recovery Testing will be conducted on a regular schedule to ensure the policy and procedures work effectively as planned. Scheduled testing may at times be contingent on resolution of technical/equipment challenges. Any lessons learned from this testing will be documented and evaluated for appropriate revisions in the Disaster Recovery policy and procedures.
  - If removable backup media is utilized it should be properly stored and properly labeled.

- All application systems and data should be prioritized for evacuation as well as disaster recovery process.
- Protect by uninterruptible power supplies all servers, backup systems, and other critical equipment from damage in the event of an electrical outage.
- Locate file servers and other critical hardware in secured rooms with Halon fire protection systems which limit damage to the immediate area of the fire. In the event of a catastrophic fire, backup data must be installed on other/replacement hardware.
- In the event of a fire or flood, turn off and unplug electrical equipment when contact with water is imminent.
- In the event of a fire or flood, seal room(s) to contain fire or water and/or use strategies to protect information and equipment from fire or from water falling from above as appropriate.
- All key staff will be trained in disaster preparation and recovery, and knowledge of responsibilities in the event of a disaster on an ongoing basis

❑ The Executive Director or designees must implement and document the following:

- Ensure that major hardware is covered under TCS's property and casualty, and or other appropriate insurance policy or policies.
- Ensure that uninterruptible power supply, fire protection, and other disaster prevention systems are functioning properly, periodically check these systems, and train employees in their use.

Priority Tasks during Emergencies:

<u>As applicable, and under appropriate circumstances, all workforce members should</u>:

- Remain calm.
- Activate the alarm. That is, pull the fire alarm or call 911 as appropriate.
- Evacuate if necessary. If personnel are injured, ensure their evacuation and call emergency assistance as necessary.
- If a fire occurs that you believe you can fight, use the nearest fire extinguisher.
- If safe, close all doors as you leave.
- Obtain portable phone(s) to communicate.
- Notify concerned fire, police, security, administration, and others as necessary.
- Notify other departments of situation and emergency protocols.
- If computers have not automatically powered down, initiate procedures to orderly shutdown systems, when possible.
- If a fire or flood occurs, disconnect power if possible and try to prevent further damage from water by covering areas with plastic sheets with adequate drainage.
- Move records/equipment/storage media away from area being flooded. Organize health information logically and label clearly for continued access.
- Arrange for transportation of paper records to a salvage, restoration, or reconstruction company.
- Respond to requests for records via portable phone rather than computer.
- Continue to provide patient charts as requested by physicians or other parties.

Priority Disaster Recovery Tasks:

<u>As applicable, and under appropriate circumstances, all workforce members should</u>:

- Prevent personnel from entering the area until officials or building inspectors have determined that the area is safe to reenter.
- Not permit unauthorized personnel to enter the affected area.
- Determine the extent of the damage and whether additional equipment/supplies are needed.
- Determine how long it will be before service can be restored, and notify departments.

- Replace hardware as necessary to restore service.
- Work with vendors as necessary to ensure that support is given to restore service.
- Notify insurance carriers.
- Retrieve and upload backup files if necessary to restore service.
- Air-dry floppy disks, if any, using a hair dryer on "air," not "heat." When dry, copy disk.
- For water damage, wipe off CD-ROMs and laser discs with distilled water, working out from the center in a straight line, and then wipe off water or dirt with a soft, dry, lint-free cloth. Air-dry. Do not use a hairdryer. For dirt or smoke damage, wipe out from the center with a clean, soft cloth. Then wash off any remaining dirt with distilled water.
- Remove water-damaged paper records by the wettest first. Freeze wet items to stabilize.
- Wrap paper records to prevent them from sticking together. Label the wrapped records.
- Contact fire, water, and storm damage restoration company. Contract for services as needed.
- Reconstruct/reacquire documents from the following:
    - Dictation system.
    - Word processing system.
    - Computer system.
    - Holders of document copies.
- Move records and equipment back to home location.
- Catch up on filing.
- Ensure that backup procedures are followed.
- Document data that cannot be recovered in patient record.
- Meet with management and staff to identify opportunities for improvement.

Additional Disaster Recovery Tasks:

The following tasks must be assigned to specific persons or positions:

- ❑ Determine whether additional equipment and supplies are needed.
- ❑ Notify vendors or service representatives if there is need for immediate delivery of components to bring the computer systems to an operational level even in a degraded mode.
- ❑ If necessary, check with other vendors to see whether they can provide faster delivery.
- ❑ Rush order any supplies and equipment necessary.
- ❑ Notify personnel that an alternate site will be necessary and where it is located.
- ❑ Coordinate moving equipment and support personnel to the alternate site.
- ❑ Bring recovery materials from offsite storage to the alternate site.
- ❑ As soon as hardware is up to specifications to run the operating system, load software and run necessary tests.
- ❑ Determine priorities of software that must be available and load those packages in order. Post these priorities in a conspicuous location.
- ❑ Prepare backup materials and return them to the offsite storage area.
- ❑ Set up operations at the alternate site if necessary.
- ❑ Coordinate activities to ensure that the most critical tasks, such as immediate patient care, are being supported as needed.
- ❑ Ensure that periodic backup procedures are followed according to our Data Backup Policy.
- ❑ Plan to phase in all critical support.
- ❑ Keep administration, medical staff, information personnel, and others informed of the status of the emergency mode operations.
- ❑ Coordinate with administration and others for continuing support and ultimate restoration of normal operations.

HIPAA-26: Contingency Operations Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs Contingency Operations planning and implementation 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 contingency operations, in accordance with the requirements at § 164.310(a) (1-2).
- Contingency Operations, for purposes of this policy document, are defined as processes and procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.
- Contingency operations plan and procedures, in combination with other emergency preparedness plans and procedures, shall be documented, analyzed, revised and updated periodically in accordance with other established emergency preparedness and documentation policies and procedures.

Policy Statement

- It is the Policy of **TCS** to be fully prepared to protect individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), during emergencies and contingency operations.
- Responsibility for planning and executing contingency operations shall reside with Executive Director, who shall prepare, review, and update plans for contingency operations on a periodic basis.
- The primary purpose of our contingency operations procedures is to allow our organization to restore lost data in the event of an emergency.
- It is the Policy of **TCS** to fully document all contingency operations plans and procedures, in accordance with our Documentation Policy.

Procedures

- Emergency and contingency plans are the responsibility of the Executive Director, who shall ensure that all such plans are up-to-date and meet our emergency preparedness requirements.
- Emergency and contingency plans, as well as data backup and disaster recovery plans shall be reviewed, and revised if necessary, at least annually. Copies of all such plans shall remain on file and be available to all personnel.
- The Executive Director shall fully document all emergency preparedness plans, including emergency and contingency plans, backup and disaster recovery plans and all the revisions thereto, in accordance with our Documentation Policy and the requirements of HIPAA.
- Service Level Agreements will be executed as needed with appropriate vendors providing any facilities, equipment or support services for the emergency and contingency plans developed.

HIPAA-27: Testing and Revision of Contingency Plans and Procedures

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs Testing and Revision of all Contingency Plans and Procedures 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 testing and revision of all contingency plans and procedures, in accordance with the requirements at § 164.308(a)(7). This includes backup and disaster recovery plans, as well as any other emergency operation plans.
- Contingency and emergency plans, as well as supporting data backup and related disaster recovery plans and the procedures associated with them, must be periodically tested and revised to ensure that they meet the emergency preparedness needs of **TCS**.
- Individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA) must be afforded the same degree of security and privacy protection during the execution of any emergency or contingency plan as such information would receive during normal business operations.

Policy Statement

- It is the Policy of **TCS** to periodically test, and revise as necessary, all emergency preparedness plans, including contingency plans as well as supporting data backup and related disaster recovery plans.
- It is the Policy of **TCS** that all individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA) shall be afforded the same degree of security and privacy protection during the execution of any emergency or contingency plan as such information would receive during normal business operations.

Procedures

- Emergency and contingency plans are the responsibility of the Executive Director, who shall ensure that all such plans are up-to-date and meet our emergency preparedness requirements.
- Emergency and contingency plans shall be tested, reviewed, and revised if necessary, at least annually. Copies of all such plans shall remain on file and be available to all personnel.
- The Executive Director shall fully document all emergency preparedness plans, including emergency and contingency plans, and all the revisions thereto, in accordance with our Documentation Policy and the requirements of HIPAA.
- Service Level Agreements will be reviewed periodically to ensure they are still appropriate to support Contingency Operation plans. This shall include all agreements with appropriate vendors providing any facilities, equipment or support services for the emergency and contingency plans developed.

HIPAA-28: Data and Applications Criticality Analyses

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs Data and Applications Criticality Analyses 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 analysis of the relative criticality of both data and applications, in accordance with the requirements at § 164.308(a)(7).
- ❑ A thorough assessment and understanding of the relative criticality of both data and applications is essential to emergency preparedness, and to effectively protecting individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA) during emergencies and during normal business operations.

Policy Statement

- ❑ It is the Policy of **TCS** to assess the relative criticality of all data, so that such data may be properly protected during emergencies and during normal business operations.

Procedures

- ❑ Data to be subject to criticality analysis shall include individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- ❑ Criticality analysis shall be the responsibility of the Executive Director or designees, who shall work in cooperation with legal counsel and other internal parties as necessary to execute and document such analyses.
- ❑ Criticality analyses shall determine and document the relative criticality of each type or category of data and applications that **TCS** possesses and/or uses to the continuity and success of our operations.
- ❑ The most critical data and applications shall be given the given the highest priority in terms of investment and emergency protection preparations; with less critical categories or types of data and applications receiving proportionately less funding and attention, as appropriate.
- ❑ In conducting data and applications analyses, the Executive Director or designees shall employ the technical guidance and recommendations of the National Institute of Standards and Technology ("NIST"), and/or other information technology "best practices", as appropriate.
- ❑ All analyses of the relative criticality of both data and applications shall be fully documented in accordance with our Documentation Policy and the requirements of HIPAA.

HIPAA-29: Evaluating the Effectiveness of Security Policies and Procedures

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs periodic Evaluations of the Effectiveness of Security Policies and Procedures 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 periodic evaluation of the effectiveness of security policies and procedures, in accordance with the requirements at § 164.308(a)(8).
- Security policies and procedures must be evaluated periodically to determine their effectiveness in appropriately safeguarding PHI.

Policy Statement

- It is the Policy of **TCS** to periodically evaluate security policies and procedures, in order to improve their effectiveness.

Procedures

- It shall be the responsibility of the Executive Director in collaboration with the HIPAA Security Officer to periodically conduct such evaluations of existing HIPAA security policies to determine need for any modifications to address new risks as well as the effectiveness of existing Administrative, Physical and Technical safeguard measures.
- Executive Director shall work in coordination with legal counsel, information technology, senior management, and any other persons, departments or parties necessary in order to conduct such evaluations.
- Such evaluations shall be conducted at least annually.
- Any updated security policies and procedures resulting from such evaluations shall be internally published and shall be available to senior management and to all parties with responsibility for safeguarding PHI.
- The purpose of such evaluations is to improve the effectiveness of our security policies and procedures, including emergency and contingency plans and procedures, so that they best protect our business, our assets, our personnel, and the individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA) that we possess or use.
- Executive Director or designee shall fully document all policy and procedure changes in accordance with our Documentation Policy and the requirements of HIPAA.

HIPAA-30: Business Associates Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs relationships with, and operations involving Business Associates 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 Business Associates, in accordance with the requirements at § 164.308(b)(1), § 164.410, § 164.502(e), § 164.504(e), and HITECH Act § 13401.
- In cooperation with our organization, Business Associates work with, use, transmit, and/or receive individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), which is afforded specific protections under HIPAA.
- **TCS** has the primary responsibility in all Business Associate relationships to ensure that individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), is properly protected and safeguarded.
- The HIPAA ("Omnibus") Final Rule specifically identifies the following types of entities as business associates which may reasonably have electronic or physical access to PHI maintained by **TCS**:
  - Subcontractors.
  - Patient safety organizations.
  - HIOs -- Health Information Organizations (and similar organizations).
  - PHRs -- Personal Health Record vendors that provide services on behalf of a covered entity.
  - Other firms or persons who "facilitate data transmission" that requires routine access to PHI.
- The "Minimum Necessary Standard" now applies directly to Business Associates. HIPAA now applies the Minimum Necessary standard directly to Business Associates and their subcontractors. When using, disclosing or requesting PHI, all these entities must make reasonable efforts to limit Protected Health Information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.
- Subcontractors of Business Associates are now Business Associates themselves. A subcontractor is defined as a person or entity to whom a Business Associate delegates a function, activity, or service involving Protected Health Information, and who is not a member of the Business Associate's own workforce.
- **TCS** is not required to enter into a contract or other arrangement with any their Business Associates subcontractors.

Policy Statement

- It is the Policy of **TCS** to establish and maintain business and working relationships with Business Associates that are in full compliance with all the requirements of HIPAA Final "Omnibus" Rule.

Procedures

- ❑ Responsibility for maintaining appropriate and lawful relationships with Business Associates shall reside with the Executive Director, who shall ensure that all aspects of our Business Associate relationships are appropriate and lawful, and who shall ensure that individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), is properly protected and safeguarded by our Business Associates.
- ❑ With regard to Business Associates, the duties and responsibilities of the Executive Director shall include, but are not limited to the following:
    - Ensure that all Business Associate contracts meet all HIPAA requirements and standards, including those requirements and standards amended by the HITECH Act, the HIPAA "Omnibus" Final Rule, and any requirements of State laws in the state(s) where we operate.
    - Ensure that individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), is properly protected and safeguarded by our Business Associates in accordance with the HIPAA Privacy and Security Rules.
    - Ensure that Business Associates understand the importance and necessity of protecting individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), whether in electronic form ("ePHI") or hardcopy form.
    - Ensure that Business Associates have proper and appropriate safeguards in place for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), before entrusting such information to them.
    - Ensure that Business Associates understand and are properly prepared to detect and respond to breaches of individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- ❑ The Executive Director shall fully document all Business Associate-related contracts and activities, in accordance with our Documentation Policy and the requirements of HIPAA.
- ❑ Business Associate Agreements will be reviewed annually for accuracy and updated as necessary. These documents will be retained for 7 years post termination of the business relationship.

HIPAA-31: Facility Security Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs Facility Security 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 facility security, in accordance with the requirements at § 164.310(a)(1-2).
- In addition to other technical and administrative safeguards, strong facility security is an essential element of our efforts to provide protection for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- It is the Policy of **TCS** to provide strong facility security, in addition to other technical and administrative safeguards, in order to provide protection for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- It is the Policy of **TCS** to fully document all facility security-related activities and efforts, in accordance with our Documentation Policy and our Maintenance Records Policy.
- It is the Policy of **TCS** to fully document facility security maintenance records-related activities and efforts, in accordance with our Documentation Policy.

Procedures

- Primary responsibility for facility security is hereby assigned to Executive Director, who shall analyze the security of our facility and implement devices, tools and techniques to strengthen our facility to a reasonable level, to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.
- A periodic analysis of our facility security controls should be included as part of the Quarterly Safety Assessment conducted by the Safety Officer. Areas of focus may include:
  - Windows and door access point
  - Electronic access control systems (i.e., Building Alarms, Video Surveillance)
  - Auditable access logs for after-hour access, if applicable
  - Routine and non-routine deliveries
- Responsibility for the creation and updating of facility security maintenance records is hereby assigned to the Security Officer, who shall establish procedures for maintaining such records in appropriate form.
- Any staff member who discovers a facility security vulnerability/risk shall bring it to the attention of the Security Officer immediately.

- **IT Equipment Security**
  - All TCS servers, and network hardware are maintained in secured, locked, environmentally conditioned rooms with 24 hour per day monitoring devices which alert the Network Administrator and/or Security Officer of any problems. Access to these rooms is limited to authorized IS and facility services workforce as required to perform job responsibilities to

maintain these rooms and/or the equipment within these rooms. Access by anyone else is granted only by approval from the Executive Director and only with an escort by an authorized IT or facility services workforce member.

- Workstations may only be accessed and utilized by authorized workforce members to complete assigned job/contract responsibilities. Third parties may be authorized by the Security Officer or Executive Director to access systems/applications on an as needed basis.
- All workforce members are required to monitor workstations and report unauthorized users and/or unauthorized attempts to access systems/applications as per the System Access Policy.
- Permanent Workstations (i.e. desktop computer, printers, and monitors) may only be moved by authorized IT workforce members.
- All wiring associated with a workstation may only be installed, fixed, upgraded, or changed by an authorized IT workforce member or other individual authorized by the Executive Director.

❑ **System/Application Access Control**

- All systems/applications purchased by **TCS** are the property of **TCS** and are distributed to users by the Information Systems staff only.
- Prior to downloading, all software must be registered to **TCS** and must be approved in advance by the Executive Director and the IT department. To prevent computer viruses from being transmitted through **TCS'**s information systems, there will be no unauthorized downloading of any unauthorized software.
- The Information Systems staff is responsible for downloading all upgrades, testing upgrades, and for supporting **TCS** systems/applications.

HIPAA-32: Workstation Use and Security Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs Information Workstation Use and Security 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 workstation use, in accordance with the requirements at § 164.310(b) and § 164.310(c).
- The establishment and implementation of an effective workstation use policy is a crucial element in our overall objective of providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- It is the Policy of **TCS** to configure, operate, and maintain our information workstations in full compliance with all the requirements of HIPAA.
- Responsibility for the development and implementation of this workstation use and security policy, as well as any procedures associated with it, shall reside with the Security Officer, in conjunction with IT personnel, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- Our objective in these efforts is to providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- Specific procedures shall be developed to specify the proper functions, procedures, and appropriate environments of workstations that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- Specific procedures shall be developed to implement physical safeguards for all workstations that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), to restrict access to authorized users only.
- It is the Policy of **TCS** to fully document all workstation use-related activities and efforts, in accordance with our Documentation Policy and the requirements of HIPAA.

Procedures

- **TCS** will have secure work areas containing workstations with physical safeguards to minimize the possibility of unauthorized observation or access to PHI. Areas where sensitive information is regularly entered or utilized will be secured using barriers to prevent public viewing of PHI.
- Only appropriate and specified work functions will be performed at secure workstations.
- If the employee accessing the sensitive information must leave the workstation at any time, it will be his or her responsibility to exit the application and/or activate the screen lock controls to remove the information being access from the workstation screen. Any hard copy records containing PHI should also be turned over, covered or re-filed before leaving.
- Printers and fax machines, copy machines, and shredders will be located in the most secure areas available, and will not be located in or near areas frequented by *members* or the public. **TCS** will also provide appropriate security measures for portable workstations containing PHI.
- All means of entry to the rooms within which employee workstations are situated will be locked when not in use.
- Employees are trained on HIPAA related policies, including workstation use and security, at the time of orientation and annually thereafter.

HIPAA-33: Device, Media and Records Disposal or Re-Use Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs Media Disposal 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 media disposal and disposition, in accordance with the requirements at § 164.310(d)(1-2).
- *Media subject to disposal* containing individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), must be completely erased, properly encrypted, or totally destroyed in its final disposition, or the data residing on such media is subject to recovery and subsequent misuse or theft.
- *Media subject to reallocation* and reuse containing individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), must be completely erased, or sanitized ("wiped") before any re-use of such media may take place, or the data residing on such media is subject to corruption, compromise, or loss.

Policy Statement

- It is the Policy of **TCS** to dispose of all media containing individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), in full compliance with all the requirements of HIPAA. This may include copiers, multi-function printers, and other devices in addition to computers, servers and other data storage systems.
- It is the Policy of **TCS** to properly erase and or sanitize ("wipe") all media containing individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), before any media may be re-used.
- It is the Policy of **TCS** to fully document all media disposal-related or media re-use and disposition-related activities and efforts, in accordance with our Documentation Policy.
- Responsibility for proper media disposal and disposition shall reside with Executive Director who shall develop procedures to ensure the proper disposition of all such media before disposal or reuse.

Key Definitions

- Degauss: Using a magnetic field to erase (neutralize) the data bits stored on magnetic media.
- Electronic Protected Health Information (ePHI): Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.
- Patient Health Information Media: Any record of patient health information, regardless of medium or characteristic that can be retrieved at any time. This includes all original patient records, documents, papers, letters, billing statements, x-rays, films, cards, photographs, sound and video recordings, microfilm, magnetic tape, electronic media, and other information recording media, regardless of physical form or characteristic, that are generated and/or received in connection with transacting patient care or business.
- Sanitization: Removal or the act of overwriting data to a point of preventing the recovery of the data on the device or media that is being sanitized. Sanitization is typically done before re-issuing a device or media, donating equipment that contained sensitive information or returning leased equipment to the lending company.

Procedures

- ❑ **TCS** has instituted an asset inventory management process to track the movement of hardware and electronic media into and out of the organization
- ❑ When devices are either transferred to another user, cycled out of use, or turned back in on lease, procedures will be employed to clear sensitive data by personnel appropriately qualified to do so and documented to provide adequate records of such action.
- ❑ All destruction/disposal of patient health information media will be done in accordance with federal and state laws and regulations and pursuant to the organization's written retention policy/schedule. Records that have satisfied the period of retention will be destroyed/disposed of in an appropriate manner.
- ❑ Records involved in any open investigation, audit or litigation should not be destroyed/disposed of. If notification is received that any of the above situations have occurred or there is the potential for such, the record retention schedule shall be suspended for these records until such time as the situation has been resolved. If the records have been requested in the course of a judicial or administrative hearing, a custody release form will be executed which states the receiving party will be responsible for returning the records to TCS, or properly destroyed/disposed of by the requesting party.
- ❑ Before reuse of any recordable and erasable media, (for example hard disks, tapes, cartridges, USB drives, smart phones, SAN disks, SD and similar cards), all ePHI must be rendered inaccessible, cleaned, or scrubbed. Standard approaches include one or all of the following methods:
  - Overwrite the data (for example, through software utilities).
  - Degauss the media.
  - Records scheduled for destruction/disposal should be secured against unauthorized or inappropriate access until the destruction/disposal of PHI is complete.
- ❑ The business associate agreement must provide that, upon termination of the contract, the business associate will return or destroy/dispose of all patient health information. If such return or destruction/disposal is not feasible, the contract must limit the use and disclosure of the information to the purposes that prevent its return or destruction/disposal.
- ❑ A record of all PHI media sanitization should be made and retained by the organization. The organization has the responsibility to retain the burden of proof for any media destruction regardless of whether destruction is done by the organization or by a contractor. Retention is required because the records of destruction/disposal may become necessary to demonstrate that the patient information records were destroyed/disposed of in the regular course of business. Records of destruction/disposal, such as a certificate of destruction, should include:
  - Date of destruction/disposal.
  - Method of destruction/disposal.
  - Description of the destroyed/disposed record series or medium.
  - Inclusive dates covered.
  - A statement that the patient information records were destroyed/disposed of in the normal course of business.
  - The signatures of the individuals supervising and witnessing the destruction/disposal.
  - Copies of documents and images that contain PHI and are not originals that do not require retention based on retention policies (e.g., provider copies, schedule print outs etc.) shall be destroyed/disposed of by shredding or other acceptable manner as outlined in this policy. Certification of destruction is not required.
- ❑ If destruction/disposal services are contracted, the contract must provide that the organization's business associate will establish the permitted and required uses and

disclosures of information by the business associate as set forth in the federal and state law (outlined in **TCS**'s HIPAA Business Associated Agreement/Contract). The BAA should also set minimum acceptable standards for the sanitization of media containing PHI. The BAA or contract should include but not be limited to the following:

- Specify the method of destruction/disposal.
- Specify the time that will elapse between acquisition and destruction/disposal of data/media.
- Establish safeguards against unauthorized disclosures of PHI.
- Indemnify the organization from loss due to unauthorized disclosure.
- Require that the business associate maintain liability insurance in specified amounts at all times the contract is in effect.

❑ Provide proof of destruction/disposal (e.g. certificate of destruction).

❑ Any media containing PHI should be destroyed/disposed of using a method that ensures the PHI could not be recovered or reconstructed. Some appropriate methods for destroying/disposing of media are outlined in the following table.

Medium	Recommendation
Audiotapes	Methods for destruction, disposal, or reuse of audiotapes include recycling (tape over), degaussing or pulverizing.
Electronic Data/ Hard Disk Drives including drives found in printers or copiers	Methods of destruction, disposal, or reuse should destroy data permanently and irreversibly. Methods of reuse may include overwriting data with a series of characters or reformatting the disk (destroying everything on it). Deleting a file on a disk does not destroy the data, but merely deletes the filename from the directory, preventing easy access of the file and making the sector available on the disk so it may be overwritten. See appendix A for links to some available software to completely remove data from hard drives.
Electronic Data/ Removable media or devices including USB drives or SD cards	Methods of destruction, disposal, or reuse may include overwriting data with a series of characters or reformatting the tape (destroying everything on it). Total data destruction does not occur until the data has been overwritten. Magnetic degaussing will leave the sectors in random patterns with no preference to orientation, rendering previous data unrecoverable. Magnetic degaussing will leave the sectors in random patterns with no preference to orientation, rendering previous data unrecoverable. Shredding or pulverization should be the final disposition of any removable media when it is no longer usable.
Handheld devices including cell phones, smart phones, PDAs, tablets and similar devices.	Software is available to remotely wipe data from handheld devices. This should be standard practice. Any removable media that is used by these devices should be handled as specified in the previous paragraph. When a handheld device is no longer reusable it should be totally destroyed by recycling or by trash compacting
Optical Media	Optical disks cannot be altered or reused, making pulverization an appropriate means of destruction/disposal.

Medium	Recommendation
Microfilm/ Microfiche	Methods for destruction, disposal, or reuse of microfilm or microfiche include recycling and pulverizing.
PHI Labeled Devices, Containers, Equipment, Etc.	Reasonable steps should be taken to destroy or de-identify any PHI information prior to disposal of this medium. Removing labels or incineration of the medium would be appropriate. Another option is to obliterate the information with a heavy permanent marker pen. Ribbons used to print labels may contain PHI and should be disposed of by shredding or incineration
Paper Records	Paper records should be destroyed/disposed of in a manner that leaves no possibility for reconstruction of information. Appropriate methods for destroying/disposing of paper records include: burning, shredding, pulping, and pulverizing. If shredded, use cross cut shredders which produce particles that are 1 x 5 millimeters or smaller in size.
Videotapes	Methods for destruction, disposal, or reuse of videotapes include recycling (tape over) or pulverizing.

- **Additional Information on Disposal of Discarded Paper Containing PHI:** Such paper copies may be disposed of in recycle bins or waste receptacles only as described below:
  1. Unsecured recycle bins/waste receptacles should be located in areas where the public will not be able to access them.
  2. When possible, dispose of paper waste containing PHI in receptacles that are secured by locking mechanisms or that are located behind locked doors after regular business hours. Locked containers must be used with copy machines located in insecure or unattended areas.
  3. Paper documents containing PHI may be placed in recycle bins/waste receptacles as described above only if the paper in such bins or receptacles will be disposed of in a manner that leaves no possibility for reconstruction of the information as described in the table above
- The methods of destruction, disposal, and reuse should be reassessed periodically, based on current technology, accepted practices, and availability of timely and cost-effective destruction, disposal, and reuse technologies and services.
- Preservation or Destruction/Disposal of Patient Health Records Upon Closure of a Provider Office/Practice will be done in compliance with HIPAA specifications.

Note; See Certificate of Data Destruction in HIPAA Policy Addendum

HIPAA-34: Hardware and Media Accountability Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs the Accountability of Information Systems Hardware and Media 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, in accordance with the requirements at § 164.310(d)(1-2).
- Proper protection of individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA), requires that we maintain records of the movements of hardware and electronic media, and any person responsible therefore.

Policy Statement

- It is the Policy of **TCS** to maintain records of the movements of hardware and electronic media containing unencrypted ePHI which are transported through third parties (this excludes third party delivery services such as FedEx, UPS, USPS, etc),in full compliance with all the requirements of HIPAA.
- Responsibility for the development and implementation of this hardware and media accountability policy, and any procedures associated with it, shall reside with the Executive Director, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- Specific procedures shall be developed to ensure that we maintain records of the movements of hardware and electronic media containing unencrypted PHI through third parties.
- It is the Policy of **TCS** to fully document all hardware and media accountability-related activities and efforts, in accordance with our Documentation Policy.

Procedures

- **TCS** has instituted an asset inventory management process to track the movement of hardware and electronic media into and out of the organization. This means that every device or media control known to the organization to house electronic PHI is identified with a unique tracking number and the disposition of each device is routinely tracked.
- Hardware which holds unencrypted ePHI that leaves the custody of **TCS**, shall be tracked by a Chain of Custody Form acknowledging custody and responsibility while in custody of 3rd party.

Note; See Chain of Custody Form in the HIPAA Policy Addendum

HIPAA-35: Unique User I.D. Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs the issuance, maintenance, and security of Unique User I.D.'s for access to **TCS**'s information systems. 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 use of unique user I.D.'s, in accordance with the requirements at § 164.306, and § 164.312(a)(1).
- The use of unique user I.D.'s is an essential element in our overall effort to protect individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- It is the Policy of **TCS** to exclusively use unique user I.D.'s for all information system access and activities, in full compliance with all the requirements of HIPAA.
- Responsibility for the development and implementation of this unique user I.D. policy, and any procedures associated with it, shall reside with Executive Director in collaboration with appropriate IT personnel, who shall ensure that access to all our information systems and data is accomplished exclusively through the use of unique user I.D.'s.
- Nothing in this policy shall limit the use of additional security measures, including login and access measures, that may further enhance the security and protection we provide to individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- It is the Policy of **TCS** to fully document all unique user I.D.-related activities and efforts, in accordance with our Documentation Policy.

Procedures

- Unique user IDs are assigned to all employees permitting password-protected role-based access to electronic PHI.

HIPAA-36: Emergency Access Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs Access to Protected Health Information during emergencies 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 emergency access procedures, in accordance with the requirements at § 164.104, § 164.306, and § 164.312(a)(1).
- The establishment of emergency access procedures further strengthens the protections we offer to individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- It is the Policy of **TCS** to establish and implement emergency access procedures, in full compliance with all the requirements of HIPAA.
- These emergency access procedures apply to access to individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- Responsibility for the development and implementation of our emergency access procedures shall reside with Executive Director, who shall ensure that these procedures are maintained, updated as necessary, and implemented fully throughout our organization.
- Specific procedures shall be developed to ensure that authorized workforce members can access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA) during emergencies.
- These Emergency Access Procedures shall be developed and implemented in combination with our emergency preparedness and response plans.
- It is the Policy of **TCS** to fully document our emergency access procedures development and implementation, in accordance with our Documentation Policy and the requirements of HIPAA.

Procedures

- Contact IT firm (CyberRisk Management) to request activation of the Disaster Recovery server at the remote DR site and initiate the associated failover process. This procedure can require up to one hour to complete for all employees.
- Contact all staff to advise them that Emergency Access procedures have be activated with instructions on access protocol.
- All administrative office staff report to disaster recovery site at the beginning of the next work day.
- Clinical staff carry on seamlessly.

HIPAA-37 Automatic Log-Off Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs the implementation of Automatic Log-Offs for **TCS**'s information systems. 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 use of automatic log-off applications, in accordance with the requirements at § 164.306 and § 164.312(a)(1-2).
- The establishment and implementation of an effective automatic log-off policy is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- It is the Policy of **TCS** to always use automatic log-off applications or systems on all workstations and computers, in full compliance with the requirements of HIPAA.
- Responsibility for the development and implementation of this automatic log-off policy, and any procedures associated with it, shall reside with Executive Director in collaboration with appropriate IT personnel, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- Specific procedures shall be developed to specify the proper functions and procedures of our automatic log-off systems on all computers and workstations that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Procedures

- **TCS** will use application and network based system configurations to enforce automatic log off/log out controls due to inactivity after a period of 5 minutes.

HIPAA-38: Encryption and Decryption Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs the Encryption and Decryption of Protected Health Information 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 encryption and decryption, in accordance with the requirements at § 164.312(a) (1-2).
- ❑ The establishment and implementation of an effective encryption and decryption policy is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- ❑ It is the Policy of **TCS** to establish and maintain this encryption and decryption policy in full compliance with all the requirements of HIPAA.
- ❑ Responsibility for the development and implementation of this encryption and decryption policy, and any procedures associated with it, shall reside with the Executive Director in collaboration with appropriate IT personnel, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- ❑ Specific procedures shall be developed to specify the proper usage and application of encryption and decryption for all computers and workstations that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- ❑ It is the Policy of **TCS** to fully document all encryption and decryption-related activities and efforts, in accordance with our Documentation Policy.

Procedures

- ❑ Encryption of Data at Rest:
  - Commercial grade data encryption technology should be installed and maintained on all mobile communication or portable storage devices (e.g., laptops, tablets, iPADS, Cell Phones, thumb drives, flash drives, etc.) which can have access to ePHI or other confidential data.
  - The use of any fileshare applications (e.g., Drop Box, Google Drive, iCloud, Microsoft OneDrive, etc.) shall not be used without approval of the Executive Director in collaboration with IT personnel. If approved for use, only client names and appointment dates/times shall be included. No PHI of any nature will be permitted. Such approval will only be granted if: 1) the filesharing need is necessary for business operations; 2) the remote parties involved have a current BAA on file; and all data is encrypted prior to sharing; or 4) the filesharing service provides commercial grade encryption and security and will sign a current BAA.
  - Off-site backup media should be encrypted at all times including any electronic transmission solution utilized.
- ❑ Data Transmission Security:
  a) Any ePHI or other confidential data shall not be sent via email or any other communications technology unless it is fully encrypted using appropriate encryption technology.
  b) Any use of other data transmission (FTP, etc.) shall not be allowed unless encryption or other appropriate security protocol has been approved by the Executive Director in collaboration with IT personnel.
- ❑ Guidelines for the use and maintenance of approved encryption technology will be communicated to all involved staff and vendors.

HIPAA-39: Audit Controls Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs Audit Controls 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 audit controls, in accordance with the requirements at § 164.312(b).
- The establishment and implementation of an effective audit controls policy is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- It is the Policy of **TCS** to establish and maintain appropriate and effective audit controls in full compliance with the requirements of HIPAA.
- Responsibility for the development and implementation of this audit controls policy, and any procedures associated with it, shall reside with the Executive Director in collaboration with appropriate IT personnel, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- Specific procedures shall be developed to specify the proper usage and application of audit controls for all computers, workstations, and systems that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- It is the Policy of **TCS** to fully document all audit control-related activities and efforts, in accordance with our Documentation Policy.

Procedures

- **TCS** will engage in semi-annual reviews of all computer systems to ensure ongoing compliance with HIPAA.
- **TCS** will perform semi-annual system configuration assessments to ensure compliance with IT security best practices (e.g., eliminate default device passwords, ensure appropriate logging and network security policies are up to date, etc.).
- **TCS** employs a role-based access system to ensure that all employees are capable of accessing only electronic PHI that is required to perform their work-related duties.

HIPAA-40: Data Integrity Controls Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs Data Integrity Controls 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 data integrity controls, in accordance with the requirements at § 164.312(c)(1-2).
- The purpose of this Integrity Controls Policy is to ensure that electronic Protected Health Information ("PHI" and "ePHI", as defined by HIPAA) has not been altered or destroyed in an unauthorized manner.
- The establishment and implementation of an effective data integrity controls policy is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- It is the Policy of **TCS** to establish and maintain appropriate and effective data integrity controls in full compliance with the requirements of HIPAA.
- Responsibility for the development and implementation of this data integrity controls policy, and any procedures associated with it, shall reside with the Executive Director in collaboration with appropriate IT personnel, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- Specific procedures shall be developed to specify the proper usage and application of data integrity controls for all computers, workstations, and systems that access individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).
- It is the Policy of **TCS** to fully document all data integrity controls-related activities and efforts, in accordance with our Documentation Policy.

Procedures

- Integrity is the process of protecting data from improper alteration or destruction during transit. Digital signatures and Message Digest (One-way Hash) both allow for the assurance that electronic PHI is truly from the sending entity and has not been modified.
- Integrity controls that focus on electronic PHI while in transit are designed to assure data is not properly modified until it reaches its appropriate destination or is disposed of. Technical solutions that assist in preserving data while in transit may include: use of firewalls, VPN's cryptography, and other authentication devices.

HIPAA-41: Person or Entity Authentication Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs Authentication of Persons or Entities seeking access to Electronic Protected Health Information in the possession 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 pertaining to person or entity authentication, in accordance with the requirements at § 164.312(d).
- The purpose of this Person or Entity Authentication Policy is to ensure that electronic Protected Health Information ("PHI" and "ePHI", as defined by HIPAA) can only be accessed by persons or entities who are in fact who they claim to be, and not imposters.
- The establishment and implementation of an effective Person or Entity Authentication Policy is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- It is the Policy of **TCS** to establish and maintain this Person or Entity Authentication Policy in full compliance with all the requirements of HIPAA.
- Responsibility for the development and implementation of this Person or Entity Authentication Policy, and any procedures associated with it, shall reside with the Executive Director in collaboration with appropriate IT personnel, who shall ensure that this policy is maintained, updated as necessary, and implemented fully throughout our organization.
- Specific procedures shall be developed to specify the proper authentication of persons and entities who request access to individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA) on our computers, workstations and systems.
- It is the Policy of **TCS** to fully document all person or entity-related activities and efforts, in accordance with our Documentation Policy.

Procedures

- Each employee is issued a unique use ID and password permitting role-based access to electronic PHI.
- Passwords are deactivated promptly for employees no longer authorized to access such information.

HIPAA-42: Data Transmission Security Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

Scope of Policy

This policy governs Data Transmission Security 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 data transmission security, in accordance with the requirements at § 164.312(e)(1) and § 164.312(e)(2).
- The purpose of our Data Transmission Security Policy and Procedures is to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.
- The establishment and implementation of effective Data Transmission Security Procedures is a crucial element in our overall objective or providing reasonable protections for individually identifiable health information, including Protected Health Information ("PHI", as defined by HIPAA).

Policy Statement

- It is the Policy of **TCS** to establish and implement technical security measures to guard against unauthorized access to Electronic Protected Health Information that is being transmitted over an electronic communications network, in full compliance with the requirements of HIPAA.
- Responsibility for the development and implementation of these Data Transmission Security Procedures shall reside with the Executive Director in collaboration with appropriate IT personnel, who shall ensure that these procedures are maintained, updated as necessary, and implemented fully throughout our organization.
- Specific Data Transmission Security Procedures shall be developed to protect individually identifiable health information, including Electronic Protected Health Information ("EPHI", as defined by HIPAA).
- It is the Policy of **TCS** to fully document all Data Transmission Security Procedures, activities, and efforts, in accordance with our Documentation Policy and the requirements of HIPAA.

Procedures

- **TCS** utilizes secure VPN (virtual private network) connections whenever transmitting electronic PHI.
- **TCS** transmits all company-based email through a secured email server.
- **TCS** utilizes email encryption for transmission of any messages or documents containing ePHI.
- Electronic PHI is permitted only in the body of secure, intra-agency emails.
- At no time is PHI permitted in the subject line of any email.
- No texting of electronic PHI without consent of the other party.

HIPAA-43 Mobile Device Policy

Effective Date:	12-01-2015	Last Revised:	12-21-2023

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.

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

Effective Date:	8-10-2015	Last Revised:	12-21-2023

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 devices that are properly configured by TCS 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.
- ❑ **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 their acceptance/acknowledgment should be documented.
- ❑ **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 no longer retain 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.

HIPAA-45 Change Control Policy, Procedure and Form

Effective Date:	7-17-2017	Last Revised:	12-21-2023

Scope of Policy

This policy governs the management of changes to the information technology infrastructure by any member of the **TCS**. All personnel of **TCS** and IT vendors 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 during the change management process.

Assumptions

- **TCS** must comply with HIPAA and the HIPAA implementing regulations, in accordance with the requirements to safeguard ePHI and provide access to patient
- Full compliance with HIPAA strengthens our ability to meet other compliance obligations, and will support and strengthen our non-HIPAA compliance requirements and efforts.
- The risk of introducing significant changes to the production environment must be managed through an appropriate level of documentation, authorization, planning, and testing. These changes could potentially impact the stability or performance of the company's IT production environment. By using a series of standardized and repeatable procedures and actions, the Company will be able to better manage any changes to the IT infrastructure in such a way that any negative impact is minimized.
- Full compliance with HIPAA reduces the overall risk to Protected Health Information (PHI), and reduces the risk to confidential health data.

Policy Statement

- Any new information system upgrade or product installation has the potential to introduce risk factors for **TCS** (e.g., system downtime, data loss and impact on patient services). This Change Control Policy requires that an orderly procedure be established for managing the risks associated with making changes to the network computing environment (i.e., Active Directory, Exchange, OS Patches, etc.), Key applications systems, and network infrastructure.
- This will be accomplished by requiring any change to be carefully assessed for potential risks and developing an appropriate contingency plan (e.g., rollback procedures) in the event something goes wrong.

Change Management Process

The process that is to be used for requesting and managing these changes is described as follows and involves defined roles:

- Roles - The following are the key roles involved in the Change Control process. One individual may be responsible for several roles as well as several individuals may be fulfilling a single role. The Executive Director is responsible for managing the execution of the Change Control process with the assistance of the HIPAA Compliance Committee.

    1. *Change Requestor* - The Change Requestor originates the request by submitting a Request For Change (RFC) to the Change Control Manager. This functional role may be filled by the manager authorizing the project and/or the IT staff person who has recommended.

2. *Change Control Manager* - The Change Control Manager (Executive Director or designee) manages the process for all requests and reviews each request for completeness. The Change Control Manager verifies that: a) the stated objectives of the request are valid; b) an acceptable risk management plan has been developed,; c) and must approve any RFC. The Change Control Manager has the discretion to deny requests that are not consistent with TCS policy or best practices.
3. *Change Implementer* - The Change Implementer makes the necessary changes as requested in the RFC and notifies any other affected parties if corresponding changes need to be made. Changes are implemented into production by the Change Implementer.
4. *Change Control Team* – In some instances, the Change Control Manager may elect to establish a Change Control Team to manage the objectives of the specific request. The team could be comprised of members representing the technical, operational and management areas. This team would meet as needed to review, approve/reject all proposed changes, and schedule change actions.

RFC Procedures: (please review and personalize as you feel appropriate for TCS)

1. A Request For Change Form (RFC) must be submitted to the Change Control Manager.
2. If the RFC is an emergency that has minimal risk impact and minimal cost, the Change Control Manager and IT staff can authorize based on a review of the RFC form; (see item 7 below). If the RFC is not an Emergency Change, an appropriate Change Control Team may be formed to review the scope and impact of the requested change.
3. An impact analysis is performed (by the Change Control Manager or a member of the Change Control Team) to determine what applications are affected by the change, if an outage is required and to determine the approximate costs and risks associated with the request. A back-out plan should also be developed and included in the impact analysis to ensure that unsuccessful changes or undesirable results do not adversely impact business processes.
4. The Change Control Team will meet as needed to review proposed changes. The Change Control Manager is the coordinator of the Change Control Team.
5. If a request is denied, the requestor is notified in writing.
6. Requests that are approved are categorized by priority (critical or normal), a Change Implementer is assigned, an implementation date is determined, and responsibility for end user communications is assigned.
7. Emergency changes and IT changes: In the event of an emergency requirement for a change, the Change Control Manager must approve a change prior to implementation and document reason for change, implementation notes and appropriate testing. The Change Control Manager will review all approved emergency changes and IT changes periodically with the IT Manager.
8. Once completed and tested, the documentation of the project and change control process shall be retained in the TCS HIPAA Documentation files.

HIPAA POLICY MANUAL ADDENDUM

Employee Acknowledgement Form

I have read, understand, and agree to comply with the HIPAA Policy and Procedures Manual. I am aware that violations of any of these Policies and Procedures may subject me to disciplinary action and may include termination of my employment subject to the Sanction Policy contained herein.

By signing this Agreement, I agree to comply with the term and conditions of this document and acknowledge that my failure to read this Agreement is not an excuse for violating it.

Employee Signature:

Printed Name	Signature	Date

Supervisor Acknowledgement:

Printed Name	Signature	Date

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

- 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

- 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.

Sanctions

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

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.

_____ _____

Employee Signature Date

_____

Employee Printed Name

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

Certificate of Data Destruction

The information described below was destroyed in the normal course of business pursuant to the organizational retention schedule and destruction policies and procedures.

Date of Destruction:	Authorized By:

Description of Information Disposed Of/Destroyed:

Inclusive Dates Covered:

METHOD OF DESTRUCTION:
Burning
Overwriting
Pulping
Pulverizing
Reformatting
Shredding
Other: _____

Records Destroyed By*:

If On Site, Witnessed By:

Department Manager:

*If records destroyed by outside firm, must confirm a contract exists

Person and Identity Verification

Person to Identify	In-Person Encounter	Telephone Encounter	Request in Writing (Fax, mail, hand-delivered)
Attorney	▪ Presents with business card and photo identification (i.e. drivers license or organization ID badge) and:	▪ It would be difficult to verify identity and authority by phone. Verification in person or in writing may be required	▪ Supplies business card, photo identification (i.e. driver's license or org ID badge), letterhead. Confirmation call is required.
Facility Directory:	▪ Verify identity	▪ Verify identity	▪ Verify identity
Patient	▪ Patient provides name, address, and date of birth and/or social security number; or ▪ Acquainted with patient	▪ Patient provides name, address, and date of birth and/or social security number; or ▪ Acquainted with patient	▪ Patient provides name, address, and date of birth and/or social security number. Verify patient's signature with that on file or on driver's license.
Personal Representative (Legal Guardian) for the Patient	▪ Personal Rep provides patient's name, address, and date of birth and/or social security number, **and** verifies (via legal docs) relationship to patient; or, ▪ Acquainted with personal Rep as such.	▪ Personal Rep provides patient's name, address, and date of birth and/or social security number, **and** verifies (via legal docs) relationship to patient; or, ▪ Acquainted with Personal Rep as such.	▪ Personal Rep provides patient's name, address, and date of birth and/or social security number. Verify the Personal Rep's signature with signature on file or on driver's license.
Persons Involved in the Patient's Immediate Care *(PHI relevant only to the patient's current care (164.510(b)).* ▪ Blood Relative ▪ Spouse ▪ Domestic Partner ▪ Roommate ▪ Boy/Girl Friend ▪ Neighbor ▪ Colleague	▪ Patient actively involves this person in his/her care; or ▪ In your best professional judgment, the disclosure is in the patient's best interest.	▪ Patient actively involves this person in his/her care; or ▪ In your best professional judgment, the disclosure is in the patient's best interest. ▪ Use call-back.	▪ N/A
Power of Attorney For the Patient	▪ Presents with a photo ID and a copy of the POA.	▪ Previously obtained a copy of the POA and verified the	▪ Obtain a copy of the POA and verify the patient's

Person to Identify	In-Person Encounter	Telephone Encounter	Request in Writing (Fax, mail, hand-delivered)
	Verify patient's signature with one on file. ▪ Acquainted with power of attorney as being such	patient's signature with one on file. ▪ Acquainted with power of attorney as being such	signature with one on file
Provider From Another Facility	▪ Acquainted with provider as a treatment provider; ▪ Provider is wearing a photo badge from his/her facility; or, ▪ Patient/personal representative introduces provider to you.	▪ Acquainted with provider as a treatment provider; or; ▪ Call requestor back through main switchboard number (not via a direct number).	▪ Recognize name of facility and address on letterhead as a treatment facility; or ▪ Call requestor back through main switchboard number (not via a direct number).
Public Official ▪ CIA ▪ Court Order ▪ FBI ▪ Law Enforcement Officer ▪ OCR ▪ OIG ▪ Public Health Agency Official ▪ Other	▪ Presents an agency I.D. badge; ▪ Presents with a written statement of legal authority; ▪ Presents with a written statement of appointment on approp. govt. letterhead; ▪ Presents with warrant, court order, or legal process issued by a grand jury, or a judicial or admin. tribunal; ▪ Presents with a contract for services or purchase order; or, ▪ Official states release is necessary to prevent or lessen the threat to the health/safety of a person/public.	▪ Official states release is necessary to prevent or lessen the threat to the health/safety of a person/public.	▪ Written statement of legal authority; ▪ Written statement of appointment on appropriate government; ▪ Warrant, court order, or other legal process issued by a grand jury or a judicial or administrative tribunal; or ▪ Contract for services or purchase order
Vendor Who Helps Assists with Treatment, Payment,	▪ Recognize requestor/ organization; or	▪ Recognize requestor or organization	▪ Recognize requestor/ organization; or

Person to Identify	In-Person Encounter	Telephone Encounter	Request in Writing (Fax, mail, hand-delivered)
or Health Care Operations Examples Include, But Are Not Limited to the Following: ▪ Accreditation Org. ▪ Insurance Co. ▪ Software Vendor	▪ Photo identification with organization		▪ Call requestor back through main switchboard number (not via a direct number).
1. **Workforce Member of Our Organization**	▪ Acquainted with individual as a workforce member; or, ▪ Workforce member is wearing an I.D. badge.	▪ Acquainted with individual as a workforce member; or, ▪ Workforce member is calling from an in-house extension.	▪ Request is sent from/through our own computer system; or ▪ Request is on our own letterhead.

PHI Disclosures Table

Requestor	Authorization Required?	Copy Fee Charged?	Track on Disclosure Accounting?
Accrediting Agencies (JCAHO, CARF)	No	No	No
Attorney for Resident	Yes	Yes	No
Attorney for Facility/Corporation	No	No	No
Contractors/ Business Associates	No, unless their purpose falls outside of TPO.	No	No
For Deceased Persons ❑ Coroner or Medical Examiner, Funeral Directors ❑ Organ Procurement	No	No	Yes
Employer ❑ PHI specific to work related illness or injury, and ❑ Required for employer's compliance with occupational safety and health laws	No, for the purpose listed. Yes for all others.	No	No
Family Members	No for oral disclosures to family members involved in care; Yes for others.	Yes	No
Entity Subject to the Food and Drug Administration ❑ Adverse events, product defects or biological product deviations ❑ Track products ❑ Enable product recalls, repairs, or replacements ❑ Conduct post marketing surveillance	No	No	Yes
Health Oversight ❑ Government benefits program ❑ Fraud and abuse compliance ❑ Civil rights laws ❑ Trauma/tumor registries ❑ Vital statistics ❑ Reporting of abuse or neglect	No	No	Yes
Health Care Practitioners and Providers for Continuity of Treatment and Payment	No	No	No
Health Care Practitioners and Providers if <u>not</u> Involved in Care or Treatment (i.e., consultants)	No	No	No
Insurance Companies/Third Party Payors ❑ Related to Claims Processing	No	No	No

Requestor	Authorization Required?	Copy Fee Charged?	Track on Disclosure Accounting?
Judicial and Administrative Proceedings ❑ Court order, or warrant ❑ Subpoena	No No - See Subpoena Policy	No Yes	Yes Yes
Law Enforcement ❑ Administrative request ❑ Locating a suspect, fugitive, material witness or missing person ❑ Victims of crime ❑ Crimes on premises ❑ Suspicious deaths ❑ Avert a serious threat to health or safety	No	No	Yes, except for disclosures to correctional institutions.
Public Health Authorities ❑ Surveillance ❑ Investigations ❑ Interventions ❑ Foreign governments collaborating with US public health authorities ❑ Recording births/deaths ❑ Child/elder abuse ❑ Prevent serious harm ❑ Communicable disease	No	No	Yes
Research (w/o Authorization)	No, if IRB or Privacy Board approves research study and waives authorization.	No	Yes
Resident/Resident's Personal Representative	No	Yes	No
Specialized Government Functions ❑ Military and Veterans' activities ❑ Protective services for the President ❑ Foreign military personnel ❑ National security and intelligence activities	No	No	Yes, except for disclosures for national security and intelligence activities.
Workers' Compensation ❑ Comply w/existing laws (see state law)	No	See applicable State Law	Yes

Request For Change (RFC) Form			
Change Action Name:			
RFC Completed By:		**Date of Request:**	
Change Type:	☐ Planned ☐ Unplanned	☐ New Installation ☐ Upgrade:	
Proposed Schedule Date		Person Responsible for Change:	
Describe Proposed Change and Purpose:			
Describe Impact on business operations (systems impacted, potential down time and for how long):			
Identify users or clients "potentially" impacted by requested change process:			
Proposed Task List (attach if already prepared, else enter steps below):			
Contingency Plan; (Describe fallback or back-out plan. Asses the adequacy of plan for reducing or eliminating risk to systems and processes to be impacted):			
Identify any Project Costs (Products/Services/Other):			
Risk Level Determination (based on severity of impact & likelihood of occurrence):			
☐ Low ☐ Medium ☐ High **Explanation:**			
Authorization: ☐ Approved ☐ Denied ☐ On Hold (explain):			
David Turner			
Printed Name	**Signature**	**Date**	
Conditions for Approval or Rejection of RFC:			

TCS Public File Share Approval Form

The use of any fileshare applications (e.g., Drop Box, Google Drive, iCloud, Microsoft OneDrive, etc.) shall not be used without approval of the Executive Director in collaboration with IT personnel. If approved for use, only client names and appointment dates/times shall be included. No PHI of any nature will be permitted.Such approval will only be granted if: 1) the filesharing need is necessary for business operations; 2) all data is encrypted prior to transmitting to fileshare and while data is stored on public share; or 3) the filesharing service provides commercial grade encryption and security and will sign a current BAA.

Requested By:		Date of Request:	
File Share Service Requested:			

Describe Purpose of Requested File Share and who needs access to share:

Describe Type of Data to be included in public file share:

Describe why this filesharing necessary for business operations:

Describe level of commercial encryption technology used to secure data in transmission and while stored in public site.

Is the vendor willing to sign a TCS Business Associate Agreement?

Identify any Service Costs:

Authorization: ☐ Approved ☐ Denied ☐ On Hold (explain):

David Turner		
Printed Name	**Signature**	**Date**

Conditions for Approval or Rejection: