CAROLINA THERAPY SERVICES

Information Technology Policies & Procedures

January 2023

INFORMATION SYSTEMS PASSWORD POLICY

PURPOSE:

The purpose of this policy is to establish a standard for the creation of strong passwords, the use and ownership of those passwords, the protection of those passwords, and the frequency with which those passwords are changed.

OVERVIEW:

This policy is administered by the Data Manager of Carolina Therapy Services, Inc.

Passwords are an important part of computer security, and often they serve as the only way to authenticate a user. Lax password procedures can compromise Carolina Therapy Services' entire information systems environment.

All Carolina Therapy Services work force members (including employees, contractors, and vendors with access to Carolina Therapy Services systems) are responsible for taking the appropriate steps, as outlined below, to select, use, and secure their passwords. All IT contractors shall be bound by this policy and implement IT policies to support it.

To the extent possible, Carolina Therapy Services will only implement systems, applications, devices, and equipment that store passwords in an encrypted format and support strong passwords. The use of strong passwords by Carolina Therapy Services work force members is required.

It is important to remember that all passwords are the property of Carolina Therapy Services and must be given to the Data Manager upon request.

SCOPE:

The scope of this policy includes all work force members who have or are responsible for a systems account (or any form of access that supports or requires a password) on any system, application, device, or other equipment, that:

- Resides at any Carolina Therapy Services location, office or facility;
- Is hosted by an application service provider;
- Has access to the Carolina Therapy Services network; or
- Stores any nonpublic Carolina Therapy Services information.

Devices subject to this policy include employees' personal smartphones, if such devices are used to access Carolina Therapy Services' network.

PROCEDURES:

General

- All system-level passwords (e.g., root, enable, admin, application administration accounts, etc.) must be changed on at least a monthly basis. Whenever the system or the application supports it, this change must be prompted by the system or application itself on an automated basis.

- All user-level passwords (e.g., e-mail, web, desktop computer, etc.) must be changed at least every quarter.

- The re-use of passwords will not be allowed.

- Users must not use the same password for gaining access to informational Web sites as they do for gaining access to Carolina Therapy Services systems or applications. Users must not use the same password for system-level and application-level access.

- Passwords must not be inserted into e-mail messages or other forms of electronic communication.

- All system-level and user-level passwords must conform to the guidelines described below.

- Default administration-level passwords that come with systems, applications, or devices must be changed immediately.

- Passwords must never be written down or stored online or on any device without encryption.

- Passwords must not be revealed to anyone, including family members, coworkers, and supervisors, except when requested by the Data Manager. Suspicions that a password has been compromised should be reported to the Data Manager immediately. If anyone other than the Data Manager asks for your password or for any other password, report him or her to the Data Manager immediately.

Password Construction Guidelines

Strong passwords having the following characteristics must be used:

- Contain both upper- and lower-case characters (e.g., a–z, A–Z).

- Have at least one digit or punctuation character (e.g., 0-9, !@#$%A&*O_+1--=\°{ }[l:°;'<>? ./)

- Are at least eight alphanumeric characters long.

- Are not words in any language, slang, dialect, jargon, etc.

- Are not based on personal information, names of family, etc.

Do not use the "Remember Password" or "Store Password" feature of any system, application, device, or equipment.

Application Development Standards

With respect to any application adopted by or developed for Carolina Therapy Services, it must be assured that such application and related programs contain the following security features:

- Authenticate individual users, not groups.
- Store passwords in an encrypted form.
- Support role management, such that one user can take over the functions of another without having to know the other's password.

The number of consecutive unsuccessful attempts to enter a correct password must be limited to three (3). After three (3) unsuccessful attempts, the involved user session must be either: (a) temporarily disabled for a minimum of three (3) minutes; (b) suspended until reset by the Security Officer or his designee; or (c) disconnected, if the involved session is a dial-up or other external network connection.

ENFORCEMENT:

All Carolina Therapy Services work force members must report any breaches or suspected breaches of this policy to the Data Manager. Any Carolina Therapy Services work force member found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or other association with Carolina Therapy Services. In addition, persons violating patient confidentiality rights or practices may be subject to civil and criminal liability under applicable law.

INFORMATION SYSTEMS AUDIT CONTROLS POLICY

PURPOSE:

The purpose of this policy is to ensure that Carolina Therapy Services, Inc. has the technical capabilities to record and examine information systems that contain or use electronic protected health information ("e-PHI").

POLICY:

It is the policy of Carolina Therapy Services to implement and use the necessary hardware, systems, applications, and procedural measures to record and examine systems activity, including access and transaction activity, in all information systems that receive, store, transmit, or otherwise access e-PHI. Carolina Therapy Services thereby can identify and investigate unauthorized data access activities. It is also the policy of Carolina Therapy Services to examine and review that recorded activity on a periodic basis, and to maintain and store such recorded activity for a reasonable amount of time. All IT contractors shall be bound by this policy and implement IT policies to support it.

PROCEDURES:

1. The Data Manager will be educated about the audit control features and functionality of the systems, applications, and devices that receive, store, transmit, or otherwise access e-PHI that are in use by Carolina Therapy Services.

2. The Data Manager will educate the appropriate work force members in charge of systems, applications, or devices that receive, store, transmit, or otherwise access e-PHI about the audit control features and functionality of their systems.

3. The Data Manger will ensure that the appropriate audit control features are turned "on" and used in all systems, applications, and devices that receive, store, transmit, or otherwise access e-PHI.

4. If systems, applications, or devices that receive, store, transmit, or otherwise access e-PHI do not have adequate audit control features and functionality, the Data Manager will so advise the President. Such systems shall be thoroughly evaluated in Carolina Therapy Services' Risk Assessment.

5. The President will consider audit control features and functionality in purchase decisions for information systems, applications, and devices that receive, store, transmit, or otherwise access e-PHI.

6. The President will ensure that adequate systems storage is available for the storage of audit control information.

7. At a minimum, the Security Officer, where feasible, will perform access and usage control audits in the following areas:

    a. Requests for Information

    b. Coding

c. Transcription

d. Modem Audits

e. Sign-in Location Audit

f. Copy/Fax Logs

g. Access to medical information by user (may be random sample of users) and patient name

8. The Data Manager will report audit control discrepancies to the President, who will determine appropriate follow-up activities.

INFORMATION SYSTEMS RISK MANAGEMENT POLICY

PURPOSE:

The purpose of this policy is to ensure that Carolina Therapy Services, Inc. complies with applicable laws regarding information systems security risk management.

POLICY:

It is the policy of Carolina Therapy Services to implement security measures sufficient to reduce risks and vulnerabilities to its information systems to a reasonable and acceptable level to comply with the requirements of HIPAA and the HITECH Act. Carolina Therapy Services will perform an assessment and manage security risks and vulnerabilities to electronic protected health information ("e-PHI"). This Risk Management policy safeguards the confidentiality, integrity, and availability of all e-PHI that Carolina Therapy Services creates, receives, maintains, or transmits; protects against reasonably anticipated threats or hazards to the security or integrity of such e-PHI; and protects against reasonably anticipated unauthorized uses or disclosures of such e-PHI. The policy will be revisited as needed, as part of Carolina Therapy Services' implementation of a continuous risk monitoring, feedback, and assessment process.

PROCEDURE:

The President of Carolina Therapy Services shall oversee and appoint a Data Manager responsible for all tasks related to information systems risk management in accordance with the policies of Carolina Therapy Services. Such risk management tasks shall include, but not be limited to:

1. Implementing security measures to reduce identified risks to information systems to reasonable and appropriate levels;

2. Monitoring security risks to all e-PHI systems throughout the year, including information systems security reviews, and providing feedback to the appropriate work force members about such risks and how to prevent, detect, respond to, and mitigate them;

3. Alerting appropriate parties as soon as possible in the event of a security threat, incident, or lapse;

4. Requiring reporting to the Data Manager and documenting, tracking, and follow-up of all defined security incidents;

5. Enforcing appropriate, standardized sanctions for violations of HIPAA security policies in coordination with Carolina Therapy Services' Human Resources Department;

6. Conducting audits of information systems activity, including logins, file access, access level modifications, and security incidents, and periodically reviewing the audit standards;

7. Periodically assessing and reporting to the President on the status of the implementation of this policy; and

8. Auditing and updating implementation of this policy no less than once per year.

INFORMATION SYSTEMS SECURITY

Carolina Therapy Services, Inc. hereby establishes the following guidelines for protecting the security of Carolina Therapy Services' information systems and information technology resources. In the absence of more detailed and specific policies and procedures covering the topical areas listed below, Carolina Therapy Services work force members should be guided in their conduct by the following considerations.

DATA SECURITY

Policy: Information will be safeguarded in a manner commensurate with its value, sensitivity, and criticality. This policy is applicable to all electronic protected health information ("e-PHI") created, collected, stored, and processed by Carolina Therapy Services. This includes any e-PHI that is the property of the organization, the patient, caregivers, researchers, and any other party, and that has been entrusted to Carolina Therapy Services for use and safekeeping. All IT contractors shall be bound by this policy and implement IT policies to support it.

CONFIDENTIALITY

Policy: Carolina Therapy Services will respect the rights of the patient with regard to the confidentiality of e-PHI. The patient is entitled to information security rights by law and regulatory requirements, as well as to any additional rights granted by Carolina Therapy Services, Inc.

Procedure: Any work force member who has access to e-PHI is responsible for maintaining the confidentiality of the e-PHI. These procedures include, but are not limited to, the following:

- taking necessary measures to preserve information confidentiality and privacy;
- maintaining a secure work environment; and
- immediately reporting any suspected breach of information security to the Data Manager.

DATA HOLDER RESPONSIBILITIES

Policy: Information system users will comply with Carolina Therapy Services' information system security controls and policies and use information assets only to execute or perform authorized patient or business functions. Users also are responsible for all work and all access occurring under their passwords. All users immediately must report to the Data Manager all actual or suspected instances of information asset theft and abuse and obvious control weaknesses affecting information security.

MANAGER RESPONSIBILITIES

Policy: Access to information will be assigned based on employee-specific job requirements. Upon any change in status (e.g., transfer, termination) of a member of Carolina Therapy Services' work force, the manager for that work force member shall provide prompt notice to the information systems administrator. Managers also are responsible for noting any deviations from policy by work force members and initiating any appropriate corrective action as a result thereof.

DATA MANAGER RESPONSIBILITIES

Policy: Carolina Therapy Services' Data Manager will monitor and audit information system usage for all of Carolina Therapy Services' systems, including but not limited to e-mail, Internet, patient care, and financial systems. Such monitoring and auditing will address issues such as inappropriate access based on identity or job description and authentication of identity. Upon discovery of any inappropriate access, the Data Manager will notify Carolina Therapy Services' Privacy Officer and assist as needed in determining whether a reportable breach occurred. The Data Manager also will maintain Carolina Therapy Services' security incident reporting and investigation process and will publish, periodically review, and revise policies, procedures, and guidelines as necessary to assure adequate information systems security.

SYSTEM SECURITY

Policy: Information systems will be safeguarded against any accidental or intentional unauthorized modification, disclosure, or destruction of e-PHI. Security measures will be employed regardless of the medium in which the information is stored, the systems that process it, or the methods by which it is moved.

Access to e-PHI will be granted and confidential information will be disclosed only to people who have a legitimate business need for it. An access request and approval process has been implemented to ensure access to information is granted appropriately; however, every individual is responsible for not attempting to access any e-PHI that they are not authorized or have no legitimate business need to access.

Passwords and User IDs will be used to safeguard systems against any accidental or intentional unauthorized modification, disclosure, or destruction of e-PHI. See Carolina Therapy Services, Inc.'s policy Information Systems Passwords for guidance on appropriate construction and use of passwords.

USE OF COMPUTING RESOURCES

Policy: Computing resources (systems, Internet, e-mail, etc.) are provided for the purpose of facilitating Carolina Therapy Services' patient care and business processes. Computing resources should not be used for any personal business, browsing, and/or disclosing of any confidential information for personal use. Any person using these resources for unauthorized or personal purposes may be subject to corrective action.

Procedure: Users should not engage in any activities that do not comply with Carolina Therapy Services' computing resources policies. These include, but are not limited to, the following:

- using computing resources for personal business;
- browsing Carolina Therapy Services information;
- disclosing any confidential information for personal use; and
- making any system changes unless authorized to do so.

PHYSICAL SECURITY

Policy: Physical access controls will be in place to ensure the security of information and information system resources as reflected in the Facility Access Controls Policy. Data processing areas, equipment,

media, and other physical computing resources containing sensitive information should be controlled. The level of control is dependent on the level of risk and exposure to loss.

Media storage devices will be cleared, purged, or destroyed in conformity with HITECH data security provisions and NIST standards, including Special Publication 800-88, Guidelines for Media Sanitization.

ENFORCEMENT

Policy: All Carolina Therapy Services work force members must report any breaches or suspected breaches of this policy to the Data Manager. Any Carolina Therapy Services work force member found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or other association with Carolina Therapy Services. In addition, persons violating patient confidentiality rights or practices may be subject to civil and criminal liability under applicable law.

INFORMATION SYSTEMS CONTINGENCY PLAN
TESTING AND REVISION POLICY

PURPOSE:

The purpose of this policy is to ensure that Carolina Therapy Services, Inc. complies with applicable laws regarding security risk analysis and mitigation.

POLICY:

Carolina Therapy Services will test the adequacy of its Contingency Plan on a periodic basis and make appropriate revisions based upon the results of and knowledge gained during the testing process.

PROCEDURES:

1. The Data Manager or designee will conduct a test of Carolina Therapy Services' Contingency Plan at least annually.

2. The Data Manager or designee will document the results of such tests.

3. The Data Manager or designee will conduct partial tests of individual components of the Contingency Plan on a regular basis.

4. The Data Manager or designee will revise the Contingency Plan as necessary.

5. The Data Manager will report to the President concerning the results of testing of the Contingency Plan.

INFORMATION SYSTEMS WORKSTATION SECURITY POLICY

PURPOSE:

To ensure that Carolina Therapy Services, Inc. minimizes the risk of unauthorized access to or disclosure of electronic protected health information ("e-PHI"), and to prevent the compromise in any way of Carolina Therapy Services' workstations that are used to create, store, access, receive, or transmit e-PHI. All IT contractors shall be bound by this policy and implement IT policies to support it.

POLICY:

Carolina Therapy Services will implement procedures that ensure the security of e-PHI by controlling access to and use of computer devices including desktop, laptop, or notebook computers ("workstations"); ensuring that workstation operating systems allow for secure log-in; and allowing for a secure unattended mode (automatic logoff or secure screensaver). Carolina Therapy Services also will ensure that workstations are protected from threats (e.g., malware, flood damage, fire, power surges), are patched appropriately, are configured to minimize the unauthorized use and disclosure of e-PHI and the installation of unauthorized software, and are properly reformatted or destroyed to remove all e-PHI before disposal or donation.

PROCEDURES:

1. The Data Manager will administer this Workstation Policy.
2. Proper workstation use and security will be a topic in the awareness and training program for all new and existing users.
3. The Data Manager will maintain an inventory of workstations.
4. The Data Manger will assess the physical placement of all workstations to ensure that:
    a. They are placed such that damage from flood, fire, and other hazards is minimized;
    b. They are physically secured if they store e-PHI on their hard drives; and
    c. They are situated such that casual observance of e-PHI on their screens/monitors is minimized.
5. The Data Manager will assess Carolina Therapy Services workstations to ensure that:
    a. They are running an operating system that allows for:
        i. Secure login;
        ii. Automatic logoff or secure screensaver; and
        iii. Encryption where required by the Risk Assessment.
    b. They have had all non-essential devices removed or disabled;
    c. Operating system patches, updates, and service packs are applied regularly;
    d. They are running appropriate anti-virus and anti-spyware software;
    e. They are free from all forms of malware;
    f. No unauthorized software is installed on them;

g. Any e-PHI that is stored on them is backed up in accordance with Carolina Therapy Services' policies; and

h. Any e-PHI that is stored on them is encrypted in accordance with Carolina Therapy Services' policies.

6. Workstations that are not owned by Carolina Therapy Services will not be used to create access, receive, store, or transmit e-PHI, and will not be placed on Carolina Therapy Services' network for any purpose without express written permission of the Data Manager.

7. Software not authorized by the Data Manager is prohibited from being installed on Carolina Therapy Services workstations.

8. Users of Carolina Therapy Services workstations will log off their system if they leave their system unattended. All Carolina Therapy Services workstations will be configured to either log off automatically or display a secure screensaver if unutilized for a period of _____ (____) minutes.

9. Users will use Carolina Therapy Services workstations according to the Information Systems Acceptable Use Policy.

10. The Data Manager will assure that prior to disposal or donation, all workstations will be reformatted or physically destroyed in conformity with the HITECH data security provisions, and NIST standards, including Special Publication 00-88, Guidelines for Media Sanitation.

11. The Data Manager will report at least semi-annually to the President concerning implementation of this policy.

ENFORCEMENT:

The Data Manager will review workstation system activity logs and audit trails to ensure compliance with this Policy. All Carolina Therapy Services work force members must report any breaches or suspected breaches of this policy to the Data Manager. Violations of this Policy may result in disciplinary action, up to and including termination of employment. In addition, persons violating patient confidentiality rights or practices may be subject to civil and criminal liability under applicable law.

INFORMATION SYSTEMS LOGIN MONITORING POLICY

PURPOSE:

The purpose of this policy is to ensure that Carolina Therapy Services, Inc. complies with applicable laws regarding the security of e-PHI through login monitoring. All IT contractors shall be bound by this policy and implement IT policies to support it.

POLICY:

Carolina Therapy Services will monitor login attempts in order to detect and report login discrepancies, such as unauthorized and/or failed login attempts and dual login attempts.

PROCEDURES:

1. The Security Officer will monitor and review login activity.
2. Work force members shall alert the Security Officer to login attempts deemed reasonably "suspect" by the work force members as soon as practicable. To the extent the implementation of such alerting is practical, Carolina Therapy Services' information systems shall alert the Security Officer automatically to login attempts classified by the system as "suspect."
3. A reasonable time of inactivity that will terminate a work force member's workstation by automatic logoff or by secure screensaver will be set by Workstation policies.
4. The Data Manager will consider a system's login monitoring and reporting functionality as a factor in Carolina Therapy Services' systems purchase decisions for those systems that require it and request that existing vendors add the functionality where it is lacking.
5. Work force members will receive training and reminders about login monitoring and reporting of discrepancies.
6. The Data Manager will report at least semi-annually to the President concerning implementation of this policy.

ENFORCEMENT:

All Carolina Therapy Services work force members must report any breaches or suspected breaches of this policy to the Security Officer. Violations of this Policy shall be grounds for disciplinary action, up to and including termination. In addition, persons violating patient confidentiality rights or practices may be subject to civil and criminal liability under applicable law.

SANCTIONS POLICY

PURPOSE:

To ensure that Carolina Therapy Services, Inc. applies appropriate sanctions for violations of its HIPAA Security Rule Policies and Procedures to discourage further such violations and to support its HIPAA Security Rule compliance program.

POLICY:

Carolina Therapy Services will apply appropriate sanctions against work force members who fail to comply with Carolina Therapy Services' HIPAA Security Rule Policies and Procedures.

PROCEDURES:

1. Carolina Therapy Services shall discipline any work force member that has not complied with its HIPAA Security Rule Policies and Procedures. Carolina Therapy Services may define specific penalties for specific security infractions. In the absence of such specific definitions, Carolina Therapy Services shall have the discretion to impose any disciplinary action for the purpose of insuring compliance, up to and including termination of employment or other association with Carolina Therapy Services.

2. Carolina Therapy Services may communicate its enforcement of sanctions for violations of security requirements to all members of its work force for the purpose of ensuring compliance.

3. Carolina Therapy Services periodically shall audit its implementation of sanctions to ensuring compliance with this policy as well as whether the severity of applied sanctions is appropriate, and it shall correct instances of inappropriate sanctions or revise the level of severity of sanctions for violations, as necessary.

4. The Data Manager and Human Resources Manager will be responsible for implementation of this policy.

5. The Data Manager and Human Resources Manager will report at least semi-annually to the President concerning implementation of this policy.

SECURITY AWARENESS AND TRAINING POLICY

PURPOSE:

The purpose of this policy is to ensure that all members of Carolina Therapy Services, Inc.'s work force are aware of and receive appropriate training on maintaining the confidentiality, availability, and integrity of electronic protected health information ("e-PHI"), as required by the HIPAA Security Regulations and the HITECH Act.

POLICY:

Carolina Therapy Services will conduct information security awareness and training activities for all members of its work force.

PROCEDURES:

1. Carolina Therapy Services will implement a security awareness and training program for all members of its work force, including employees, management, independent health care providers, and vendors or contractors working onsite who have access to e-PHI in Carolina Therapy Services' information systems.

2. Such awareness and training activities will include periodic security updates and reminders, procedures for guarding against, detecting, and reporting malicious software, procedures for monitoring log-in attempts and reporting discrepancies, and procedures for creating, changing, and safeguarding passwords.

3. Training may be implemented in any practical way including in person, via webcast, and e-mail updates provided that a mechanism is implemented for ensuring that the trainee completes the training.

4. All new members of Carolina Therapy Services' work force will undergo security training within 30 days of being hired. Individuals having access to e-PHI will be trained before they begin their duties for Carolina Therapy Services.

5. Carolina Therapy Services will maintain written records of security training.

6. Carolina Therapy Services will review its training procedures regularly and specifically following any revisions or additions to applicable laws and regulations regarding information security or confidentiality of e-PHI.

7. The Data Manager will report at least semi-annually to the President concerning implementation of this policy.

ENFORCEMENT:

Any work force member found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or other association with Carolina Therapy Services. In addition, persons violating patient confidentiality rights or practices may be subject to civil and criminal liability under applicable law.

SECURITY INCIDENT PROCESS

PURPOSE:

The purpose of this policy is to ensure that Carolina Therapy Services, Inc. and all members of its work force effectively identify, document, and report information security incidents and respond to such incidents appropriately.

POLICY:

Carolina Therapy Services requires that every member of its work force report, and Carolina Therapy Services will respond to, information security incidents that have the potential to allow unauthorized access, disruption, or damage to or theft of information security resources, including electronic protected health information ("e-PHI"). Appropriate incident response will include mitigation activities that reasonably limit the impact on Carolina Therapy Services' information systems due to an incident, and investigative activities that facilitate a resolution of such incident. All IT contractors shall be bound by this policy and implement IT policies to support it.

PROCEDURES:

1. Carolina Therapy Services will implement procedures for addressing information security incidents. Such procedures will:

    a. Enable Carolina Therapy Services to monitor and respond to security incidents 24 hours per day, seven days per week;

    b. Define the process for reporting information security breaches and the individual to whom such breaches should be reported;

    c. Describe the process for investigating such breaches, the persons to be involved in the investigation, and the appropriate timetable for concluding the investigation;

    d. Describe the process for response and follow-up to the investigation, including attempted mitigation, discipline of those found responsible for the breach, and any revision of security practices deemed necessary due to the breach;

    e. Describe the process for alerting appropriate authorities in the event that there is an information security threat, incident, or other lapse in information security;

    f. Describe the process for determining whether the security incident constitutes a breach of unsecured PHI, as required by the HITECH Act; and

    g. Maintain documentation of each security incident, including the type of incident; the results of the investigation; the measures taken to mitigate the breach and to prevent future recurrences of such a breach; and any discipline taken against the person(s) responsible for the breach.

2. Carolina Therapy Services will test its security incident reporting and response mechanism regularly to determine its effectiveness.

3. Carolina Therapy Services will comply with State and Federal breach notification laws, including the HITECH breach notification requirements, as applicable.

4. The Data Manager will report at least semi-annually to the President concerning implementation of this policy.

TRANSMISSION SECURITY POLICY

PURPOSE:

To ensure that Carolina Therapy Services, Inc. secures electronic protected health information ("e-PHI") against improper alteration, destruction, or unauthorized interception during transmission.

POLICY:

Carolina Therapy Services will implement safeguards for transmitting e-PHI to minimize the risk of improper alteration, destruction or unauthorized interception during transmission. Such safeguards will address the risk of message interception and interpretation by parties other than the intended recipients. These safeguards also will protect information systems from intruders attempting to exploit external communications points. All IT contractors shall be bound by this policy and implement IT policies to support it.

PROCEDURES:

1. Carolina Therapy Services will have integrity controls to ensure the validity of the information sent or received. Through the use of check sums, double keying, message authentication codes, or digital signatures or encryption algorithms, as appropriate, such controls will corroborate that e-PHI has not been altered or destroyed.
2. Carolina Therapy Services will implement a mechanism to encrypt e-PHI whenever deemed appropriate. Transmissions of e-PHI across an open network (*e.g.*, the Internet) will be encrypted such that only the recipient can interpret them, unless the patient or patient's representatives authorizes in writing an unencrypted transmission. Encryption processes shall comply with the National Institute of Standards and Technology ("NIST") or similar Federal Information Processing Standards 140-2 validated standards outlining valid encryption processes that comply with the HITECH security provisions, including NIST Special Publications 800-52, Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations; 800-77, Guide to IPsec VPNs; and 800-113, Guide to SSL VPNs, as applicable.
3. Carolina Therapy Services will require integrity controls for any information technology upgrades or purchases.
4. The Data Manager will report at least semi-annually to the President concerning implementation of this policy.

ENFORCEMENT

All Carolina Therapy Services work force members must report any breaches or suspected breaches of this policy to the Security Officer. Any Carolina Therapy Services work force member found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or other association with Carolina Therapy Services. In addition, persons violating patient confidentiality rights or practices may be subject to civil and criminal liability under applicable law.

HIPAA SECURITY COMPLIANCE EVALUATION POLICY

PURPOSE:

The purpose of this policy is to ensure that Carolina Therapy Services, Inc. complies with applicable laws regarding evaluation of its HIPAA Security compliance.

POLICY:

Carolina Therapy Services will review all HIPAA Security Policies and Procedures for technical and non-technical viability, effectiveness, and compliance with the HIPAA Security Rule at least on an annual basis. Carolina Therapy Services will evaluate its overall HIPAA Security Rule compliance plan at least on an annual basis.

PROCEDURES:

1. The Data Manager will be responsible for insuring Carolina Therapy Services practices and procedures comply with the HIPAA Security Rule by considering:

    a. Changes in the HIPAA Security or Privacy Regulations;

    b. New federal, state, or local laws and regulations affecting HIPAA;

    c. Changes in the risk management process;

    d. Changes in Carolina Therapy Services' IT environment;

    e. Changes in Carolina Therapy Services' business processes with respect to IT; or

    f. A significant security incident occurs.

2. The Data Manager will periodically review the current HIPAA Security Rule Policies and Procedures and invite work force members to offer feedback, comments, and other input regarding Carolina Therapy Services' HIPAA Security Rule Policies and Procedures.

3. When necessary, the Data Manager will update the Policies and Procedures to ensure compliance with the HIPAA Security Rule.

4. The Data Manager may ask the President to request assistance from Carolina Therapy Services' counsel in complying with this policy.

5. The Security Officer will report at least semi-annually to the President concerning implementation of this policy.

DEVICE AND MEDIA CONTROLS POLICY

PURPOSE:

The purpose of this policy is to manage the receipt and removal of hardware and electronic media into and out of Carolina Therapy Services, Inc. and within Carolina Therapy Services to maintain the confidentiality of the electronic protected health information ("e-PHI") contained on such media.

POLICY:

Carolina Therapy Services has established procedures governing the receipt and removal of hardware and electronic media that contain e-PHI into and out of Carolina Therapy Services, and Carolina Therapy Services monitors the movement of these items within Carolina Therapy Services' operation, as described below. All IT contractors shall be bound by this policy and implement IT policies to support it.

PROCEDURES:

1. Carolina Therapy Services will appropriately dispose of electronic media and devices that store e-PHI.

    a. Computer hardware and old tapes, diskettes, hard drives, and other media storage devices, when ready for disposal, will be physically destroyed consistent with National Institute of Standards and Technology ("NIST") Special Publication 800-88, Guidelines for Media Sanitation, such that they can never be used again and e-PHI cannot be retrieved from the devices.

    b. The Data Manager or designee periodically will review and update Carolina Therapy Services' data disposal processes.

2. Before any media, including tapes, diskettes, hard drives, and USB devices are reused, the Data Manager or his designee will remove e-PHI from all such media by making the data unreadable or unrecoverable consistent with NIST Special Publication 800-88, Guidelines for Media Sanitation.

3. No removable device (including cell phones and tablets) or media shall be used to store e-PHI without written authorization from the Data Manager. All removable devices or media that store e-PHI must be encrypted. The Data Manager will maintain an inventory of all removable hardware and electronic media that stores e-PHI. Included in this inventory will be the individuals responsible for these devices and media when they are removed from or moved within Carolina Therapy Services.

4. Workforce members who accessed e-PHI using personal devices, including cell phones and tablets, will be required to allow Carolina Therapy Services to access or control their device at any time, including, if necessary, to wipe all data from the device. Workforce members must also submit their personal devices to the IT department for removal of any e-PHI prior to termination of employment.

5. The IT department will establish procedures for ordering, receiving, distributing, installing, and disposing of hardware and software, consistent with NIST guidelines and the HITECH Act security provisions.

6. The Data Manager will report at least semi-annually to the President concerning implementation of this policy.

ENFORCEMENT:

All Carolina Therapy Services work force members must report any breaches or suspected breaches of this policy to the Data Manager. Any work force member found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or other association with Carolina Therapy Services. In addition, persons violating patient confidentiality rights or practices may be subject to civil and criminal liability under applicable law.

FACILITY ACCESS CONTROLS POLICY

PURPOSE:

The purpose of this policy is to ensure that Carolina Therapy Services, Inc. protects information security resources by outlining minimally acceptable physical security practices, controlling access to its information resources, and managing access for those persons performing repairs on Carolina Therapy Services, Inc.'s information systems equipment.

POLICY:

Carolina Therapy Services, Inc. maintains facility access controls that safeguard Carolina Therapy Services, Inc.'s facility and its information security resources from unauthorized access, as described below. All IT contractors shall be bound by this policy and implement IT policies to support it.

PROCEDURES:

1. Carolina Therapy Services, Inc. has implemented procedures to limit physical access to its electronic information systems and to the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed during appropriate hours and during times of disaster recovery. Such procedures:
    a. Safeguard the facility from unauthorized physical access and safeguard the information systems equipment from unauthorized physical access, tampering, and theft, both after normal business hours and during business hours by unauthorized individuals;
    b. Require the use of physical mechanisms to control access to buildings and/or computer facilities, such as surveillance cameras, keys, tokens, and combinations;
    c. Establish procedures regarding the physical and information security access of visitors, including where applicable, maintenance of a visitor log, positive identification check, and an information technology authorization check before visitor access is approved;
    d. Ensure that persons testing and performing repairs on Carolina Therapy Services, Inc.'s information systems equipment are only allowed access to that equipment or those systems being tested or repaired;
    e. Require regular auditing and monitoring of these physical mechanisms for facility and system security breaches;
    f. Include a procedure for sanctioning security breaches, and maintain a record of such breaches and the manner in which Carolina Therapy Services, Inc. responded to each; and
    g. Identify one person to be responsible for maintaining and updating the facility security plan.
2. Carolina Therapy Services, Inc. maintains records documenting repairs or modifications to the facility (e.g., hardware, walls, doors, locks) and evaluates the effect of any repairs or modifications upon the facility security plan.

ENFORCEMENT:

All Carolina Therapy Services, Inc. work force members must report any breaches or suspected breaches of this policy to the Data Manager. Any work force member found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or other association with Carolina Therapy Services, Inc. In addition, persons violating patient confidentiality rights or practices may be subject to civil and criminal liability under applicable law.

INFORMATION SYSTEMS CONTINGENCY PLAN

PURPOSE:

The purpose of this policy is to ensure that Carolina Therapy Services, Inc. maintains an information systems Contingency Plan to address Carolina Therapy Services operations in the event of interruptions to the critical functions of Carolina Therapy Services' information systems.

POLICY:

Carolina Therapy Services will maintain a Contingency Plan addressing the steps that must be taken to maintain business critical functions in the event of losses, disruptions, or disasters affecting Carolina Therapy Services' facilities and/or information systems.

PROCEDURES:

1. The Contingency Plan will be maintained by the Data Manager and include strategies to ensure the contingency of information systems.
2. As part of the Contingency Plan, the Data Manager will also oversee a data backup plan to restore data in an emergency or other occurrence (*e.g.*, fire, vandalism, system failure, cyberattack, or natural disaster) that may damage or compromise its information systems.
3. The Contingency Plan will also establish emergency operations procedures to address continuing operations of information systems in the event of various emergencies.
4. The Data Manager will conduct periodic testing of the Contingency Plan and revise the plan if necessary.
5. The Data Manager will report at least semi-annually to the President concerning implementation of this policy.

INFORMATION SYSTEMS ACCEPTABLE USE POLICY

OVERVIEW:

This policy sets forth, **in general terms**, Carolina Therapy Services, Inc.'s practices for use of and access to Carolina Therapy Services' IT resources. This policy references additional specific policies, which must be read and acknowledged in conjunction with this policy. The lists of activities below are by no means exhaustive, but attempt to provide a general framework for activities that fall into the category of acceptable and unacceptable use.

AUTHORITY:

This policy is administered by the Data Manager of Carolina Therapy Services. The intent of this Acceptable Use Policy is both to inform and to protect Carolina Therapy Services' IT users (work force members, subcontractors, consultants, and trading partners), and Carolina Therapy Services from illegal or damaging actions by IT users.

PURPOSE:

The purpose of this policy is to outline the acceptable use of Carolina Therapy Services' IT resources—including, but not limited to: computer products, equipment, and systems, including desktop/notebook computers, peripherals, tablets, and other portable devices, medical/lab equipment and devices, software applications, operating systems, telephone systems, storage media, and network accounts providing e-mail and Internet access. All IT contractors shall be bound by this policy and implement IT policies to support it.

Breaches of this policy could challenge the confidentiality, integrity, and availability of data handled by Carolina Therapy Services' IT resources by exposing Carolina Therapy Services to risks, including virus attacks, "hacking" attacks on our network systems, and intentional/unintentional unauthorized disclosure of protected health information ("PHI") or electronic protected health information ("e-PHI"). Breaches of this policy could expose Carolina Therapy Services to legal and regulatory actions.

SCOPE:

This policy applies to all IT users at and IT resources owned by Carolina Therapy Services.

POLICY:

Ownership

1. All IT resources and all messages and other data composed, sent, received, or stored on these systems are and remain the property of Carolina Therapy Services. Carolina Therapy Services reserves the right to audit and monitor usage of these resources, and to access, view, and disclose their contents, with or without notice to or the consent of the IT user, in accordance with the requirements of HIPAA and any other applicable laws

and regulations. These IT resources are provided to Carolina Therapy Services work force members primarily to serve the interests of Carolina Therapy Services and of its patients in the ordinary course of business. The Data Manager will report at least semi-annually to the President concerning implementation of this policy.

General Security and Proprietary Information

IT users must take all necessary steps to prevent the unauthorized disclosure of and unauthorized access to sensitive and confidential information, including e-PHI, on any Carolina Therapy Services IT resource. IT users must keep passwords secure in accordance with the Information Systems Password Policy. IT users must comply with all Carolina Therapy Services Information Systems policies and procedures at all times.

- All IT resources used by IT users that are connected to the Carolina Therapy Services. Internet/Intranet/Extranet, whether owned by the IT user or Carolina Therapy Services shall be continually executing approved virus-scanning software with a current virus database.

- Any IT resource owned by Carolina Therapy Services and used at an IT user's home or other location must be used in accordance with this Acceptable Use Policy and all other Information Systems policies and procedures, and may be so used only with permission of the Data Manager.

Unacceptable Use

Under no circumstances is an IT user of Carolina Therapy Services authorized to engage in any activity that is illegal under local, state, federal, or international law while utilizing any IT resource owned by Carolina Therapy Services.

The following activities are, in general, prohibited (certain IT users may be exempted from these restrictions during the course of their legitimate job responsibilities, as approved by the Data Manager):

- Acts that violate the rights of any person or company protected by copyright or other intellectual property, including the installation, use, or distribution of technology products/services for which Carolina Therapy Services does not own a license.

- Using any of Carolina Therapy Services' IT resources to engage in obtaining or forwarding material that is in violation of sexual harassment or hostile workplace laws, including but not limited to pornographic material.

- Unauthorized copying of any and all copyrighted materials for which Carolina Therapy Services or the IT user does not have an active license.

- Unauthorized copying of confidential data (specifically including e-PHI) without permission from the Security Officer.

- Making IT resources available to unauthorized IT users.
- Using any IT resource for personal gain.
- Exporting software or technical information in violation of international or regional export control laws.
- Introducing any nonapproved application software or other programs (malicious or not) into any IT resource owned by Carolina Therapy Services without the permission of the Data Manager.
- Transporting data by any means to one's home, except when using a Carolina Therapy Services laptop computer or other device.
- Revealing one's account password or other authentication method to others or allowing use of one's account by others, including family members.
- Circumventing user authentication or security of any IT resource.
- Making fraudulent offers of products or services originating from any Carolina Therapy Services account.
- Causing disruption, congestion, or security breaches of network communications. Security breaches include, but are not limited to, accessing data that the IT user is not authorized to access or logging into a server or account that the IT user is not expressly authorized to access.
- Port scanning or security scanning, unless approved by the Data Manager.
- Executing any form of IT resource monitoring which will intercept data not intended for the IT user's use, unless this activity is a part of the employee's normal job/duty.
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, an IT resource owned by Carolina Therapy Services.

ENFORCEMENT:

All Carolina Therapy Services work force members must report any breaches or suspected breaches of this Acceptable Use Policy to the Data Manager. Any work force member found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or other association with Carolina Therapy Services. In addition, persons violating patient confidentiality rights or practices may be subject to civil and criminal liability under applicable law.

INFORMATION ACCESS MANAGEMENT POLICY

PURPOSE:

The purpose of this policy is to ensure that Carolina Therapy Services, Inc. maintains information access controls on its information systems to know, at any given time, which work force members may view or disclose electronic protected health information ("e-PHI").

POLICY:

Carolina Therapy Services has established information access controls on its information systems to protect e-PHI and other information from unauthorized viewing, modification, or disclosure, as described below. All IT contractors shall be bound by this policy and implement IT policies to support it.

PROCEDURES:

1. The Data Manager will oversee Carolina Therapy Services' information access procedure that grants access to e-PHI based upon job classifications specifying the minimum level of information access required to perform each job.
2. The Data Manager, in conjunction with the Human Resources Manager, will determine who may access e-PHI in the event of contingency or disaster recovery operations.
3. The Data Manager will oversee the maintenance of records of all work force members' level of access to information security systems, based upon each individual's verified work-related need for access to e-PHI. Such records must be updated every time an individual's level of access to e-PHI is changed. These records will be periodically audited to ensure their accuracy.
4. Every work force member must undergo training before gaining access to e-PHI.
5. Each work force member must acknowledge in writing his or her understanding and acceptance of the responsibility that accompanies the grant of access to e-PHI.
6. Individual work force members' access to e-PHI will be changed as a result of administrative actions (employee transfer, change in job description), and access to all information systems resources will be terminated promptly in the event of an employee's termination or resignation. Following termination, Carolina Therapy Services will conduct an exit interview and ask whether the employee was aware of any information security breaches.
7. The Data Manager will report at least semi-annually to the President concerning implementation of this policy.

ENFORCEMENT

Policy: All Carolina Therapy Services work force members must report any breaches or suspected breaches of this policy to the Data Manager. Any Carolina Therapy Services work force member found to have violated this policy may be subject to disciplinary action, up to and including termination of employment or other association with Carolina Therapy Services. In addition, persons violating patient confidentiality rights or practices may be subject to civil and criminal liability under applicable law.

COMPUTER AND INFORMATION USAGE POLICY
AND AGREEMENT

Each person holds a position of trust when accessing data and resources of Carolina Therapy Services, Inc. and must recognize the responsibility to preserve the security and confidentiality of this information. Therefore, all persons who are authorized to access data and resources, both through Carolina Therapy Services, Inc.'s information systems and through individual local area networks and databases, must read and comply with Carolina Therapy Services' policies.

Those who cannot follow these standards of behavior may be denied access to Carolina Therapy Services' computer systems and networks. Persons violating these standards may be subject to penalties, including disciplinary action under Carolina Therapy Services' policies and under federal and state laws.

The following specific principles apply to all Carolina Therapy Services staff, employees, physicians, volunteers, students, faculty, and contractors regardless of their job classification or position. Each of these persons agrees to:

- Respect the privacy and rules governing the use of any information accessible through the computer system or network and only utilize information necessary for performance of my job.
- Respect the ownership of proprietary software. For example, I will not make unauthorized copies of such software for my own use, even when the software is not physically protected against copying.
- Respect the finite capability of the systems, and limit my own use so as not to interfere unreasonably with the activity of other users.
- Respect the procedures established to manage the use of the system.
- Prevent unauthorized use of any information in files maintained, stored, or processed by Carolina Therapy Services.
- Not seek personal benefit or permit others to benefit personally by any confidential information or use of equipment available through my work assignment.
- Not operate any non-licensed software on any computer provided by Carolina Therapy Services.
- Not exhibit or divulge the contents of any record or report except to fulfill a work assignment and in accordance with Carolina Therapy Services policy.
- Not knowingly include or cause to be included in any record or report a false, inaccurate, or misleading entry.
- Not remove or copy any record or report from the office where it is kept, except in the performance of my duties.

- Not download any record or files onto a laptop, USB flash drive, or other portable device, except in the performance of my duties. I further agree to safeguard any such portable device against theft or unauthorized access.

- Report any violation of this policy.

- Understand that the information accessed through all Carolina Therapy Services' information systems contains sensitive and confidential patient care, business, financial, and employee information that should only be disclosed to those authorized to receive it.

- Not release my authentication code or device to anyone else, or allow anyone else to access or alter information under my identity.

- Not use anyone else's authentication code or device in order to access any Carolina Therapy Services system.

- Respect the confidentiality of any reports printed or copied from any information system containing patient information and handle, store and dispose of these reports appropriately.

- Not divulge any information that identifies a patient except as permitted by Carolina Therapy Services policies and applicable law.

- Understand that all access to Carolina Therapy Services system will be monitored.

- Understand that my obligations under this Agreement will continue after termination of my work at Carolina Therapy Services. I understand that my usage privileges are subject to periodic review, revision, and if appropriate, renewal.

By signing this, I agree that I have read, understand, and will comply with this Policy and Agreement.

_____ _____

Signature Date

_____

Printed Name

Disciplinary Action Policy for Lost, Stolen, or Damaged Company Issued Equipment

Table of Contents

1. Background

CTS Employees are directed to understand the disciplinary process as it pertains to the focused issue of information technology within the larger scope of the disciplinary process as found within the CTS Policies and Procedures and the Employee Handbook.

2. Purpose

The purpose of this policy is to define the disciplinary process and actions for any employees who are assigned CTS owned equipment that is lost, damaged, or stolen. This disciplinary policy applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

- IPads
- IPhones
- Laptop Computers
- Tablet Devices
- Mobile Phones
- Cellular Computing Devices (ex. MIFI)
- Ultra-mobile PCs (UMPC).
- Any mobile device capable of storing corporate data and connecting to an unmanaged network.

3. Disciplinary Actions

The following disciplinary actions are agreed upon by CTS and the CTS Employee or end-user of the assigned equipment:

IPad/Tablet Damage/Loss/Theft

- 1st Infraction..... Write-Up & Warning
- 2nd Infraction..... Write-Up & $250 replacement fee
- 3rd Infraction..... Dismissal & $250 replacement fee

Laptop Damage/Loss/Theft (Computers that are 0 – 2 years-old)

- 1st Infraction..... Write-Up & Warning
- 2nd Infraction..... Write-Up & $150 replacement fee
- 3rd Infraction..... Dismissal & $150 replacement fee

Laptop Damage/Loss/Theft (Computers that are 2+ years-old)

- 1st Infraction..... Write-Up & Warning
- 2nd Infraction..... Write-Up & $50 replacement fee
- 3rd Infraction..... Dismissal & $50 replacement fee

Desktop Damage/Loss/Theft (Computers that are 0 - 2 years-old)

- 1st Infraction..... Write-Up & Warning
- 2nd Infraction..... Write-Up & $200 replacement fee
- 3rd Infraction..... Dismissal & $200 replacement fee

Desktop Damage/Loss/Theft (Computers that are 2+ years-old)

- 1st Infraction..... Write-Up & Warning
- 2nd Infraction..... Write-Up & $50 replacement fee
- 3rd Infraction..... Dismissal & $50 replacement fee

IPhone/Android/Mobile Phone Damage/Loss/Theft

- 1st Infraction..... Write-Up & Warning
- 2nd Infraction..... Write-Up & $200 replacement fee
- 3rd Infraction..... Dismissal & $300 replacement fee

Mobile Devices with Data Plans including, IPhone/IPad Use Overages

- 1st Infraction..... Verbal Warning
- 2nd Infraction..... Write-Up & Warning
- 3rd Infraction..... Write-Up & Overage Fees

General IT Violations Beyond Equipment Damage/Loss/Theft

- 1st Infraction..... Verbal Warning
- 2nd Infraction..... Write-Up, Warning & Suspension w/o Pay
- 3rd Infraction..... Dismissal

CAROLINA THERAPY SERVICES

EMPLOYEE AGREEMENT

_____ _____

EMPLOYEE'S NAME (PLEASE PRINT) DATE (MM/DD/YYYY)

_____ _____

POSITION/JOB TITLE FACILITY(FACILITIES)

I _____ have read the Carolina Therapy Services Acceptable Use Policy. I am familiar with its contents. I agree to abide by these guidelines and understand the enforcement thereof. I understand that my use of the CTS network, workstations, laptops, mobile devices, & printers may be monitored.

EMPLOYEE SIGNATURE: _____ DATE:_____

On this date, _____, I have received a laptop/workstation/mobile device with the following serial and model information:

Serial Number: _____ Model: _____ Tag:_____

Serial Number: _____ Model: _____ Tag:_____

Serial Number: _____ Model: _____ Tag:_____

Serial Number: _____ Model: _____ Tag:_____

I understand, having read the Carolina Therapy Services Acceptable Use Policy that I am responsible for all electronic equipment that I have been issued. I agree that at the end of my employment, voluntary or otherwise, to return all equipment issued to CTS immediately in good working order. I understand that CTS reserves the right to collect the replacement value of any devices in the event it is not returned, or is returned in an inoperable or damaged condition.

EMPLOYEE SIGNATURE: _____ DATE:_____

MANAGER SIGNATURE: _____ DATE:_____

DIRECTOR SIGNATURE: _____ DATE:_____