HIPAA AND ELECTRONIC DEVICES

- This inservice is a summary of the Carolina Therapy Services Information Technology Policy and Procedure Manual. A copy of this full manual will be placed in each CTS department.

ACCEPTABLE USE

- CTS Information Technology refers to all personal and company-owned computer/electronic devices used for CTS purposes, data, applications, and the supporting networking infrastructure.
- IT is a vital part of our documentation and delivery of patient services, human resources, and our continuing education:
  - All client information and treatment plans are electronically created and stored
  - All full-time therapy staff receive an electronic device to conduct client-centered care
  - Every facility and clinic has internet access

ACCEPTABLE USE

- This policy establishes guidelines for acceptable use of CTS-provided information resources. It includes examples of what you can do and what you can not do and what rights you have. Guidelines are based on the following principles:
  - Information resources are provided to support the essential mission of CTS
  - CTS policies and state and federal law that govern use of information resources
  - You are expected to use information resources with courtesy, respect, and integrity
  - The IT infrastructure is provided for the entire company. It is finite and requires a large financial commitment to maintain. All users are expected to use it responsibly.
  - Because an action is easy to do does not mean it is legal or appropriate

ELECTRONIC COMMUNICATION

- Pertains to emails, text messages, faxes, and other forms of electronic messaging
- All communication must be compliant with the Health Insurance Portability and Accountability Act of 1996 (HIPAA)
- Emails transmitted across a network should never be considered fully private or confidential. Consider them to be electronic postcards – viewable by anyone
- CTS respects the contents of saved files to electronic devices. The IT dept does monitor the corporate network and will comply with lawful orders of courts (subpoenas, search warrants, etc) to access copies of system files, email content, or other information.

RESPONSIBILITIES

1. Protecting IT Resources from Physical Access – You must control unauthorized use of your corporate information resources by preventing others from obtaining access.
2. Protecting IT Resources from Electronic Access – You must protect your information resources from unauthorized electronic access by using effective passwords and by safeguarding those passwords.
3. Using Electronic Communications Responsibly – CTS electronic communications should be used for corporate-related activities in an ethical and responsible manner – free of patient names and other identifying information.

All stored electronic correspondence belongs to CTS. It should be considered private and confidential unless CTS or an authorized agent has explicitly made it available to others. Any destruction, modification, or deletion of company property or stored information will result in counseling.

RESPONSIBILITIES

4. Use of Personal Electronic Devices – Personal devices should be locked away with other personal property in a secure location and are discouraged from being used in the workplace. Personal cell phones and other devices should be turned off during the workday unless approved in writing by the Area Director. Under no circumstances should a personal electronic device be used to communication, record, or store protected patient health information, patient photographs, patient videos, etc. Recording, storing, and/or transmitting protected health information, patient photographs/videos, etc must be done on company-owned equipment, be accompanied with any appropriate waiver signed by the patient/POA, and done with the approval of the company President.

RESPONSIBILITIES

5. Using Limited Resources Responsibly, Efficiently, and Fairly – Network resources must be used in an efficient and fair manner. It is not responsible to use disproportionate amounts of IT resources (ex: peer-to-peer applications, streaming media at high bit rates, serving a multi-user online game, etc).

6. Complying with the Terms of the User Agreement- CTS staff are expected to read, understand, and comply with the terms of the agreement you acknowledge annually. Refer to the CTS IT Director with any questions.

7. Complying with CTS Rules and Federal Laws – CTS staff are expected to comply with all applicable corporate regulations and federal and state laws.

CTS reserves the right to terminate computing services of users who violate rules or infringe on rights of copyright holders and proceed with disciplinary action up to and including termination

REQUIREMENTS

- You are the only person who can use an information resource that CTS has provided for your personal use.
- NEVER GIVE YOUR PASSWORD TO ANYONE, even people that you trust. If you suspect someone may have discovered or guessed your password, it must be changed.
- You are responsible for excessive charges accrued using the computing account or resources assigned to you, even if a friend using your account without your permission runs up the charges

REQUIREMENTS

- Be civil when using electronic media. Never send rude or harassing correspondence. If someone asks you to stop communicating with them, you should. If you feel that YOU are being harassed, the HR dept will assist you.
- Do not interfere with activities of others or use a disproportionate share of IT resources.
  - Sending unsolicited messages to a large number of recipients (spamming)
  - Consuming an unauthorized/disproportionate share of networking resources
  - Deliberately causing any denial of service including flooding, ICMP attacks, etc.

REQUIREMENTS

- Never use or disclose protected health information, data, or other confidential information, without appropriate authorization.
  - Only share protected health information (PHI) via an encrypted source
  - Make sure any individual with whom you share PHI is authorized to receive the info
  - Do not share or store PHI data with anyone not associated with the care or billing of services for that patient
  - Do not share corporate business data that may be classified as PHI data (ex: status of negotiations, terms of contracts, etc)
  - Comply with corporate agreements to protect vendor information such as software code, pricing, etc
  - If you receive a request for PHI data from a third party outside of CTS, notify your Area Director
  - Immediately report violations of CTS policies to your Area Director

SOCIAL COMPUTING AND NETWORKING

- Online social networking opportunities include professional blogs, communities, wikis, peer-to-peer file sharing networks and other channels of online discussion and interactive publishing.
- CTS respects the rights of employee personal privacy outside of the workplace, however any employee publication, interaction, or online representation that references CTS is covered by this policy.
- Employees are responsible for everything they publish online and should exercise good judgement in determining whether the information they release is professional, appropriate, and representative of CTS.

SOCIAL COMPUTING AND NETWORKING

- In general, interactions with online communities or interactive publishing media must:
  - Identify the employee by name and organizational role in any communications or publications about CTS
  - Be accompanied by a disclaimer that any views expressed are the employee's own and are not endorsed by or representative of CTS
  - Provide value in all interactions
  - Adhere to principles of conduct and professionalism that govern other in-person and workplace communications. Do not publish abusive, harassing, defamatory, obscene, etc content.
  - Comply with conduct guidelines and applicable laws and contractual terms (see manual)

SOCIAL COMPUTING AND NETWORKING

- The following may not be disclosed on social media without explicit consent of CTS:
  - Conversations between employees
  - Announcements, documents, discussions or other info shared in internal meetings
  - Names of clients, partners, suppliers, or other employees
  - Internal emails, notes, memos, and other interpersonal communications
  - Internal documents not marked for external distribution
  - Pre-publication drafts of documents ultimately intended for public distribution
  - Planning/production documents or software code
  - Organizational charts
  - Contracts, policies, intellectual property of CTS, or other legal documents

INTERNET USE AND MONITORING

- The IT dept monitors internet use from all computer and devices connected to the corporate network.
- General trending and activity reports will be made available to any employee as needed upon request. IT, Operations, and administration team may access all reports and data if necessary to respond to a security incident.
- Please refrain from visiting any site on your assigned device that you are not using for CTS-related purposes.

PASSWORD POLICY

- Passwords are an important aspect of protection of equipment and protected patient information.
- Strong passwords have the following characteristics:
  - Contain at least three of the following character classes:
    - Lower case characters
    - Upper case characters
    - Numbers
    - Punctuations
    - “Special” characters (@#$%^(){}, etc.)
  - Contain at least fifteen alphanumeric characters

PASSWORD POLICY

- Weak passwords have the following characteristics:
  - Less than 15 characters
  - The password is found in the dictionary
  - It is a common-usage word
    - Names of family, pets, friends, fantasy characters
    - Computer terms
    - The words “Carolina”, “Therapy”, “Services” or any derivation
    - Birthdays, addresses, or phone numbers
    - Word or number patterns (aaabbb, qwerty, zyxwvuts, 123321, etc)
    - Any of the above spelled backwards
    - Any of the above preceded or followed by a digit (ie: secret1)

PASSWORD POLICY

- Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title or other phrase. For example “This Might Be One Way To Remember” and the password would be TmB1w2R!
- Do not share passwords with anyone, including administration. All passwords are to be treated as sensitive, confidential CTS information.
- Passwords should never be written down or store online without encryption
- Do not reveal a password in email, chat, or other communication
- Do not hint at the format of a password (ie: “family name”)
- Do not reveal a password on questionnaires or security forms.
- Always decline the “remember password” option on websites and applications
- If someone asks you for your password, refer them to the IT policy and IT Director.

WORKSTATION AND EQUIPMENT SECURITY

- Employees are responsible for maintaining the physical security of CTS computer resources under their control and for protecting the integrity and privacy of the data maintained on them by appropriate use of lockdown devices, password controlled access, etc.
- CTS reserves the right to inspect all data and to monitor the use of all its computer systems. Users have no right to privacy on CTS-owned equipment.
- CTS’s right of access to personally owned computing devices will be limited to CTS’s patient or business information.

WORKSTATION AND EQUIPMENT SECURITY

- All CTS equipment must be secured to protect against damage
- All CTS equipment must be secured with appropriate updated software for detecting the presence of malicious software
- All workstations must be positioned or located in a manner that will minimize the exposure of any displayed PHI or business information. When necessary, privacy screens can be deployed.
- Users accessing CTS devices from remote locations (such as a home location) should employ appropriate security safeguards.
- Users may not independently install connectivity hardware or software to the computing resources of CTS.

WORKSTATION AND EQUIPMENT SECURITY

- Users are required to log-off of applications containing PHI or business information before leaving their workstations
- When the user chooses to save work containing PHI to the computer or to a portable unit (ie: flashdrive), it has to be encrypted.
- In the event that a critical document or file is deleted, contact the IT director. DO NOT CONTINUE TO USE THE WORKSTATION.
- All laptops and devices must be secured when not in use. Security may be provided by locking the equipment in a cabinet, desk, office, etc. This is the employee's responsibility. In some cases, it may be necessary to take your ASSIGNED computer home at the end of the day – a signed AUP must be on file with the HR dept.

WORKSTATION AND EQUIPMENT SECURITY

- All CTS workstations and devices must utilize a password screen saver or PIN number access screen. Any exceptions must be approved in writing by the Area Director.
- All systems containing PHI or business information must employee auto log-off capabilities, if available.
- Upon termination or change of job position, users will have network access removed or modified immediately.
- All devices owned by CTS shall be tagged and tracked by the IT dept.
- Installation of personal software (screensavers, gifs, etc) is prohibited. Any software must be approved and installed by the IT dept.
- The loss or theft of any CTS-owned device must be reported immediately.

DISCIPLINARY ACTIONS

- CTS staff are directed to understand the disciplinary process as it pertains to the focused issue of IT within the larger scope of the disciplinary process as found within the CTS

- Applies to any employee assigned a CTS-owned laptop, iPhone, iPad, or any other electronic device

DISCIPLINARY ACTIONS

iPad Damage/Loss/Theft

- 1st infraction: Write up and warning
- 2nd infraction: Write up and $250 replacement fee
- 3rd infraction: Dismissal and $250 replacement fee

iPhone and Droid Damage/Loss/Theft

- 1st infraction: Write up and warning
- 2nd infraction: Write up and $200 replacement fee
- 3rd infraction: Dismissal and $300 replacement fee

Laptop Damage/Loss/Theft

- 1st infraction: Write up and warning
- 2nd infraction: Write up and $150 replacement fee (0-2 years old), $50 (2+ years old)
- 3rd infraction: Dismissal and $150 replacement fee (0-2 years old, $50 (2% years old)

Desktop Damage/Loss/Theft

- 1st infraction: Write up and warning
- 2nd infraction: Write up and $200 replacement fee (0-2 years old), $50 replacement fee (2+ years old)
- 3rd infraction: Dismissal and $200 replacement fee (0-2 years old), $50 replacement fee (2+ years old)

MAJOR POINTS

- It is EVERYONE'S responsibility to secure their CTS-issued electronic equipment
- It is EVERYONE'S responsibility to use devices appropriately
  - No personal devices used in the dept unless approved by AD
- It is EVERYONE'S responsibility to abide by HIPAA regulations in all communications and interactions
  - No patient names, photos, videos, insurance numbers or other identifying information or protected company information in emails, texts, or postings to social media
- There are consequences for breach of CTS policy or damage/loss of equipment

FOR QUESTIONS OR ISSUES

- Katie Neal
  - katien@carolinatherapy.net
  - 910-892-0027
- Chastity Strickland, HR Director
  - chastitys@carolinatherapy.net
  - 910-892-0027