HIPAA Privacy & Security Training

HIPAA

The Health Insurance Portability and Accountability Act of 1996

AMTA confidentiality requirements

- AMTA Professional Competencies
  - 20. Documentation
    - 20.7 Demonstrate knowledge of professional Standards of Clinical Practice regarding documentation. (5.3.3 Place such documentation in the client's file and maintain its confidentiality unless proper authorization for release is obtained.)
  - 22. Professional Role/Ethics
    - 22.12 Apply laws and regulations regarding the human rights of the clients.

AMTA confidentiality requirements

- AMTA Code of Ethics
- **3.0 Relationships with Clients/Students/ Research Subjects**
  - **3.12 Confidentiality**
    - 3.12.1 The MT protects the confidentiality of information obtained in the course of practice, supervision, teaching, and/or research.

AMTA confidentiality requirements

- AMTA Code of Ethics
- 3.12.5 All forms of individually identifiable client information, including, but not limited to verbal, written, audio, video and digital will be acquired with the informed client or guardian consent and will be maintained in a confidential manner by the MT. Also, adequate security will be exercised in the preservation and ultimate disposition of these records.

CBMT Scope of Practice

- IV. B. Professional Responsibilities

  7. Maintain client confidentiality within HIPAA privacy rules.

HIPPA: The Health Insurance Portability and Accountability Act of 1996- Privacy Rule

- Gives consumers increased control over their PHI.
- Sets boundaries on the use and disclosure of health records.
- Establishes safeguards to protect privacy of health care information.
- Holds violators accountable with civil and criminal penalties.
- Balances public responsibility when health care information must be released to protect the public.

HIPPA: The Health Insurance Portability and Accountability Act of 1996- Privacy Rule

- The concept of HIPAA's Privacy and Security Regulations is simple:
  - KEEP INDIVIDUALS' HEALTH INFORMATION SECURELY CONFIDENTIAL

Definitions

- HEALTH INFORMATION.--The term 'health information' means any information, whether oral or recorded in any form or medium, that--”
- (A) is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and”
- (B) relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of health care to an individual.

Definitions

- "(6) INDIVIDUALLY IDENTIFIABLE HEALTH INFORMATION.--The term 'individually identifiable health information' means any information, including demographic information collected from an individual, that--”
  - (i) identifies the individual; or”
  - (ii) with respect to which there is a reasonable basis to believe that the information can be used to identify the individual.

What is Protected Health Information?

Identifiable information refers to information that that could be used to identify the patient:

- Individual's name, address, phone/fax numbers, email address
- Employer's name, certificate/license number, voice or fingerprint data
- Relative's names, photos, date of birth •
- Social Security number, medical record number, membership or account numbers

Definitions

- "(2) SAFEGUARDS.--Each person … who maintains or transmits health information shall maintain reasonable and appropriate administrative, technical, and physical safeguards--"
  - (A) to ensure the integrity and confidentiality of the information;
  - "(B) to protect against any reasonably anticipated--"
    - (i) threats or hazards to the security or integrity of the information; and"
    - (ii) unauthorized uses or disclosures of the information

Why is HIPAA important for students?

- **The HIPAA rules for privacy and security will apply to you when you are assigned as an observer or student in the MTC and affiliated organizations engaged in providing health care services, such as schools, hospitals, group homes, nursing homes and mental health centers.**

HIPAA Security Rule

HIPAA Security Rule

- Effective April 21, 2005
- Safeguards electronic PHI
- Covers:
  - Information stored on:
    - Hard drives
    - Disks (CD-RW's, DVD's)
  - Information transmitted through e-mail, Internet, or other means

HIPAA Security Rule

- Faxes and voice transmissions
  - Generally, detailed PHI is NOT to be released over the telephone even if disclosure is permitted or authorized.
  - PHI should NOT be faxed, even if disclosure is authorized or permitted
  - All faxed PHI shall include a fax coversheet explaining that the information being faxed is confidential and should be destroyed if not received by the intended recipient.

What is Information Security?

- The protections in place to ensure PHI is kept confidential, is not improperly altered or destroyed, and is available for those who are authorized to access it.
- The Music Therapy program and MTC Information Security includes the following:
  - Hardcopies of documentation
  - Computer hardware
  - Software
  - Information security/practice policies

Documentation Hardcopies

- Should never have client's names on them, a first initial only is recommended.
- Should not be left where they can be found or read by anyone other than you or your supervisor. This includes in your parked and locked car.
- Are to be kept in a locked cabinet at the MTC
- Should be shredded when your corresponding course at EMU is completed.

Passwords

- Are essential in protecting information.
- Should never be given to anyone including supervisors, friends, and fellow students.
- Should not be stored in a desk, or written on a sticky note and put on a computer.

How to choose a password

STRONG passwords:

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters (e.g., 0-9, !@#$%^&*()_+|~- = \‘{}[]:";’<>?,./)
- Are at least eight (8) alphanumeric characters long
- Are not based on personal information, names of family, names of pets, etc.

Physical Security

- Staff, contractors, etc. are given access to the MTC rooms on an as needed basis.
- The MTC computer should be logged off when not in use
- Computers should not be placed where anyone other than authorized users can see what is on the screen. This means when you are using your computer in a public place, or using a public computer and doing documentation.
- When using a public computer, do not put a copy from your flashdrive onto the public computer
- Close the browser when done if submitting material electronically from a public computer

Electronic Media

- Disks and other media should be sent to the IT department for destruction.
- Do not throw away old media. Data can still be recovered even if files were deleted.
- The use of encrypted and password protected USB drives to store PHI should be used.
- Encrypt your USB drive BEFORE saving information on it or the info will be lost.

E-mail Use & Transmission of Data

- Any identifying consumer information is not allowed in e-mail. This includes consumer initials, consumer ID's, date of birth, address, etc.
- Data should not be sent via e-mail without being encrypted (ZixMail, digital certs, etc).

Offsite Security

- When working at home, printing of any demographic or clinical documents containing consumer information is strictly prohibited.
- Laptops/Tablets should not be left unattended and should be password protected.
- PDA’s/Smart Phones must be password protected.

Level One – Carelessness

- The unintentional disclosure of PHI.
- Examples:
  - Leaving PHI in a public area at work, vehicle, home office, etc.
  - Inadvertent disclosure of identifying consumer information via email, public computer screen, etc.
  - Inadvertent verbal disclosure of identifying consumer information
- Sanction – At a minimum, corrective action plan and training.

Level Two – Improper Access Without Disclosure

- Unauthorized use or misuse of PHI.
- Violation of “Minimum Necessary” provisions:
  - Maintaining pictures or other identifying consumer information on a computer hard drive (consent issue)
  - Must be on password protected flashdrive or CD-ROM
- Sanction – A potential minimum of a written reprimand, and could be up to suspension

Level Three – Improper Disclosure

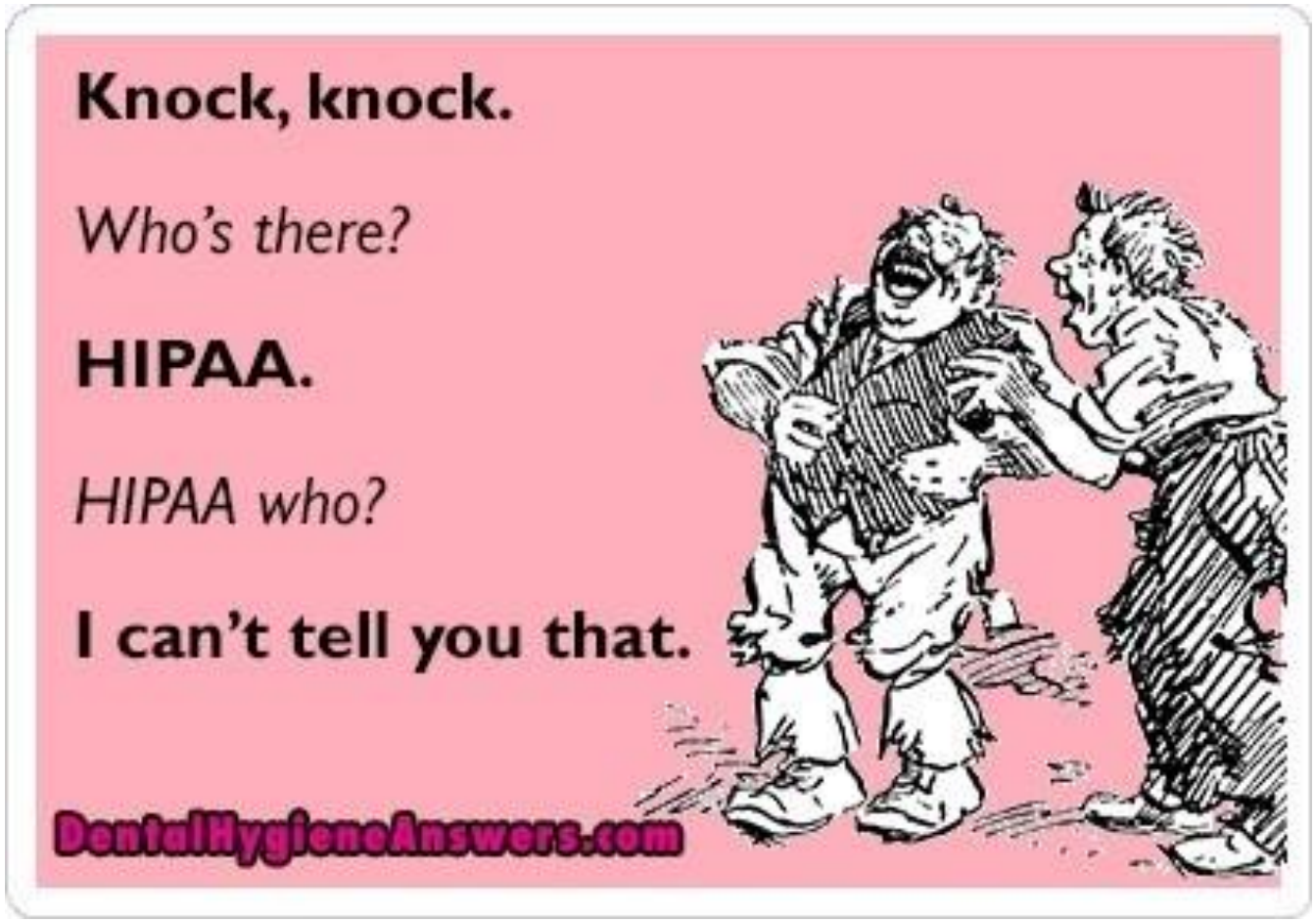
- The willful or intentional disclosure of PHI; deliberately obtaining PHI for malicious reasons.
- Examples include:
  - Compiling mailing lists for personal use or to sell
  - Obtaining PHI to get information for malicious reasons
  - Disclosing PHI without an appropriate consent
- Sanction – Violations on this level could potentially result in permanent dismissal

Violations and Noncompliance

- What is a violation?
  - Inappropriately accessing or releasing information, whether intentional or unintentional.
- Federal Penalties for noncompliance
  - Misuse of PHI include fines up to $50,000/ imprisonment for a term of up to one year.
  - Misuse under false pretenses includes fines up to $100,000/imprisonment for a term of up to five years.
  - Misuse with intent to sell, transfer, or use PHI for commercial advantage includes fines up to $250,000/imprisonment for a term up to 10 years.

So, what does this mean to you?

- It is your responsibility to:
  - Protect our clients' PHI.
  - Respect the rights of our clients.
  - Protect the program from risk of PHI use or disclosure violation.
  - Report violations and/or security breaches immediately.


Knock, knock.
Who's there?
HIPAA.
HIPAA who?
I can't tell you that.
DentalHygieneAnswers.com