MINOT STATE UNIVERSITY

Department of Communication Disorders
Communication Disorders Clinic

Health Insurance Portability and Accountability Act of 1996 (HIPAA)

PURPOSE:

To provide protection for the privacy of certain individually identifiable health information, referred to as **Protected Health Information (PHI),** such as: client's name, address, and social security number.

** In general, it is intended to ensure **Client Confidentiality** for all health care related information.

HIPAA **Privacy Rule** provides standards for protecting the privacy of health information. The Privacy Rule also:

- Gives clients more control over their health information;
- Sets boundaries on the use and release of health records;
- Establishes appropriate safeguards that the majority of health-care providers and others must achieve to protect the privacy of health information;
- Holds violators accountable with civil and criminal penalties that can be imposed if they violate client's privacy rights;
- Strikes a balance when public health responsibilities support disclosure of certain forms of data;
- Enables clients to make informed choices based on how individual health information may be used;
- Enables clients to find out how their information may be used and what disclosures of their information have been made;
- Generally limits release of information to the minimum reasonably needed for the purpose of the disclosure;
- Generally gives clients the right to obtain a copy of their own health records and request corrections and
- Empowers individuals to control certain uses and disclosures of their health information.

Privacy Rule

What does the privacy rule require?

- Intended to protect privacy of "protected information"
- Creates new compliances for "covered entities", which include all health care providers, all health plans, all health information clearinghouses and those "business associates" who engage directly or through contractual arrangements with any of the above
- Transactions include all **Electronic Data Interchange (EDI)** such as electronic claims, payment from third party payers, coordination of benefits information, health plan eligibility as well as direct discussions between individuals and fax transmissions
- Also covers all paper files containing protected information which has not yet been transferred to electronic format (all information on clients – hard and soft files)
- MSU-CDC must obtain client consent for most disclosures of PHI

Clients' privacy rights under the privacy rule are as follows:

- Right to know that private, individually identifiable health care information will remain protected and not be disclosed to anyone without their authorization except where explicitly permitted by the rule
- Right to receive a copy of the "**Notice of Privacy Policies**" produced by MSU-CDC
- Right to request that the release of their information be restricted to specific individuals and entities of their choice
- Right to know who has had access to their protected information
- Right to access their protected information and amend the record in instances where they feel the information is missing or is in error
- Right to file a complaint with the HHS office of Civil rights about any rights that have been denied by MSU-CDC

Security Procedures

All information must be safeguarded!

1. PAPER
    a. All documents must remain in the client's record
    b. NO copies are permitted
    c. Documents containing client's health information must be shredded

2. ORAL
    a. All conversations concerning a client must take place in a private room
    b. Only discuss client's with those directly involved
    c. Don't discuss the clients with the secretaries
    d. Don't leave messages on answering machines unless client has granted permission on Patient Record of Disclosures

e. Make phone calls to clients in private areas
f. Call clients by only their first names in the waiting room
g. Counsel clients only in a private area

3. VISUAL
    a. View records in a private room
    b. Computer screens must be protected
    c. Audio and video tapes are considered medical media and must be stored in a safe place and erased at the end of the semester

4. REPORT WRITING
    a. Reports may only be saved to password protected folders… NEVER save on an unprotected hard drive
    b. Drafts must be shredded immediately

De-identifying Information

Occasionally client information may be used for academic assignments or research purpose. In these cases, approval to use client information must be granted by the appropriate Communication Disorders Department faculty member. For therapy and diagnostic clients the clinical supervisor is authorized to grant permission. If the clinical supervisor is no longer employed in the department, the Clinic Director may grant permission. For research purposes, the faculty member directing the research or chairing the thesis committee may grant permission. The completed "Permission to De-Identify and Use Client Information" form must be completed and presented to the Clinic Operations Manager before the student is allowed access to client files.

To De-identify Client Information

Remove ALL information which may identify the client:

- Name
- Relatives
- Employers
- Birthdates - Addresses
- Zip codes
- County
- City
- Date of admission - Etc.

Do NOT just black out information with a marker as it may still be visible

Sanctions for Violations

** Sanctions can range from a **Warning** to **Termination** from the program. Sanctions will vary based on the severity of the action, whether the action was intentional or unintentional, and

whether or not the action represents a pattern or practice of behavior. **All violations**, not just repeat offenses, **will be sanctioned**.

Appropriate responses will be determined on a case-by-case basis. Responses to violations will depend on a number of factors including the severity of the violation and the record of the student. For example, while an inadvertent violation might normally result in additional training of policies/procedures, it could result in more serious action if it was part of a pattern of violations or other performance problems.

Examples of Violations:

- Failure to lock up protected health information (PHI) or follow other safeguard provisions
- Inadvertently throwing papers containing PHI in regular garbage rather than shredding it
- Telling friends about your irritating client and that he or she has HIV (or any other personal medical information)

** **Students** who are engaged in clinical experiences giving them access to protected health information will be subject to discipline, up to and including termination from the clinical practicum. If the student is enrolled in a class, he/she will be subject to grading consequences according to the judgment of the instructor/supervisor.

The following **Violation Levels** will be considered in determining the appropriate sanctions:

LEVEL 1

Failing to demonstrate appropriate care and safeguards in handling PHI. These are usually unintentional with no improper disclosure of the information. **Examples** of Level 1 violations may include:

- Failing to log-off system
- Leaving individually identifiable information unattended in a non-secure area
- Failure to lock up PHI
- Inadvertently throwing papers containing PHI in regular garbage rather than shredding it
- Sending/faxing information to an incorrect address
- Other minor first-time violations of policies

LEVEL 2

Intentional or unintentional exposure of PHI to internal inappropriate access, unauthorized access to individually identifiable health information, or repeated Level 1

violations. These result in no improper further disclosure inside or outside the University setting. **Examples** of Level 2 violations may include:

- Sharing ID/passwords with other students/staff that result in internal inappropriate access
- Accessing individually identifiable health information for which the individual has no responsibility or which is needed as part of assigned duties
- Talking about clients in areas where others might hear
- Failure to obtain appropriate consent to release information
- Failure to fulfill training requirements

LEVEL 3

Intentional or unintentional disclosure of PHI information inside or outside the University setting, or repeated Level 2 violations. **Examples** of Level 3 violations may include:

- Providing passwords to unauthorized individuals that result in disclosure outside the University
- Sharing of PHI with unauthorized individuals
- Telling friends about your irritating client and that he or she has HIV (or any other personal medical information)
- Failing to perform the necessary responsible actions that would prevent disclosure of individually identifiable health information
- Accessing the record of a friend or family member out of curiosity without a legitimate need to know the information

LEVEL 4

Intentional abuse of PHI. **Examples** of Level 4 violations may include: -
Large-scale disclosures of individually identifiable health information

- Using PHI for personal gain
- Altering, tampering with, or destroying PHI

Levels of Access to Client Files/Documents

- **Observers in CD 310, 322, 420** ○ NO access to client files or documents. Information may be obtained through the supervisor or the clinician being observed.

- **Observers in CD 324** ○ Access to client files or documents through approval by the course instructor.

- **Student Clinicians (therapy and diagnostics)** ○ Access to the file, working file and other documents may be granted for the clinician's current client(s) only.

- May have access to previous client information only with supervisor approval. If previous supervisor is unavailable, Clinic Director may grant approval.

- **Supervisors** ○ Access to clients whom they are supervising or clients supervised in the past.

- **Non-supervising faculty** ○ Access to client files with approval of the Clinic Director or Department Chair.