The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law (Public Law 104-191) passed by Congress to improve the portability and continuity of health insurance coverage; to facilitate uniform electronic commerce and electronic data interchange; to combat waste, fraud, and abuse in health insurance and health care delivery; to simplify the administration of health insurance; and to guarantee security and privacy of health information. There are four components of the law:

1. Privacy Standards
2. Security Standards
3. Electronic Transaction and Code Sets
4. National Provider and Employer Identifiers

The law requires covered healthcare components to implement appropriate administrative, physical, and technical safeguards to avoid unauthorized use or disclosure of individually identifiable health information. Agencies are instructed to use reasonable safeguards and protections that are flexible.

HIPAA set forth various civil and criminal penalties for violations of the law:

**Civil Penalties (Health and Human Services):** Fines up to $100 per violation; maximum of $25,000 in each calendar year for identical violations

**Criminal Penalties (Department of Justice): - Three Degrees**
- **Knowing misuse of information:** fines up to $50,000 and/or prison of up to 1 year.
- **False pretenses:** fines up to $100,000 and/or prison of up to 5 years.
- **Personal gain or malicious harm:** fines up to $250,000 and/or prison term of up to 10 years.

**HITECH Act**
Under Title XIII of the American Recovery and Reinvestment Act of 2009 called the Health Information Technology for Economic and Clinical Health (HITECH) Act, many of the requirements of HIPAA are expanded to increase the security of individually identifiable health information. The HITECH Act’s enhanced privacy and security standards are applicable to both healthcare components and those doing business with healthcare components when individually identifiable health information is involved.

**Covered Entity**
A “covered entity” is a healthcare organization that maintains or transmits protected health information (PHI) electronically in connection with a standard transaction. Each covered entity shall maintain reasonable and appropriate administrative, technical, and physical safeguards (A) to ensure the integrity and confidentiality of the information; and (B) to protect against any reasonably anticipated threats or hazards to the security or integrity of the information and unauthorized uses or disclosures of the information; and (C) otherwise to ensure compliance with this part by the officers and employees of such person.

A “hybrid entity” is an organization whose main function is not healthcare, but portions of that organization are covered under HIPAA. A hybrid entity must identify its covered components and ensure compliance with the regulations.
Protected Health Information (PHI)
Protected Health Information is the personal, individually-identifiable medical data that relates to a client’s health, the provision of health services, and the payment for health services. PHI includes a broad range of medical information relating to any individual and covers information regarding communication disorders. Protected Health Information is any information that can identify an individual which is used or held by a health insurance organization. The information includes: name, address, phone number, date of admission or discharge, date of birth, email address, social security number, diagnosis, or medication. PHI can be transmitted or maintained electronically, written, or orally. The Notice of Privacy Practices explains how the Appalachian State University Communication Disorders Clinic may use PHI.

Transactions
A covered transaction is the exchange of information between two parties to carry out financial or administrative activities related to health care, such as health care claims or equivalent encounter information, health care payment and remittance advice, coordination of benefits, enrollment and disenrollment in a health plan.

If a covered entity conducts a covered transaction with another covered entity using electronic media, the covered entity must conduct the transaction using standard formats, code sets, and data elements.

Disclosure
Disclosure is the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

Privacy of Health Information
The HIPAA privacy regulations apply to covered entities that transmit health information in electronic covered transactions. These regulations protect individually identifiable health information that is created or maintained in any form by those covered entities. A covered entity may not use or disclose protected health information (PHI) except as permitted or required under HIPAA.

Under the HIPAA Privacy regulations, individuals (with few exceptions) have the right to:
- Receive a Notice of Privacy Practices
- Request restrictions on uses and disclosures of PHI
- Access their PHI
- Amend their PHI
- Receive an accounting of PHI disclosures

Workforce
Any individual employed by the covered entity and who has access to an individual’s protected health information is considered to be a part of the workforce. In the Communication Disorders Clinic this would include: any speech-language pathologist or audiologist authorized to enter information in a clinic chart; all departments and units of the Communication Disorders Clinic; all students, both graduate and undergraduate, majoring in Communication Disorders at Appalachian State University; any member of a volunteer group allowed to help in the Communication Disorders Clinic (for example, a public school employee who is working with a
child in the preschool program may be able to view a chart); and all employees, staff, and other clinic personnel, authorized by the Communication Disorders Clinic Privacy Official, including contractors or other entities directly involved with clients in the clinic.

**Research**
A covered entity may use or disclose PHI for research if the covered entity obtains authorization from the individual(s) described by the PHI or a waiver of the authorization from an institutional research board. The data also may be used if all individual identifiers have been removed from the data. A graduate student is allowed to discuss a client in class as long as no identifying information is given in the discussion.

**Business Associates**
A business associate is a third party to which a covered entity provides PHI in the “course of business;” a person or entity who performs certain functions, activities, or services for a covered entity, involving the use of PHI, and who is not a member of the covered entities workforce. A covered entity may disclose PHI to a business associate and may allow a business associate to create or receive PHI on its behalf if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. These assurances must be written in a contractual agreement.

Under the HITECH Act business associates are required to comply directly with the Privacy and Security Rule provisions directing implementation of administrative, physical, and technical safeguards for electronic protected health information. A business associate must report any breaches to the covered entity.

**Security Requirements**
The HIPAA security regulations apply to covered entities that process an electronic transmission between entities or electronically maintain health information that has been or will be sent to or received from another covered entity. The security regulations require:

- Administrative procedures to manage and protect the data
- Physical safeguards for computers, buildings, and equipment related to fire, natural and environmental hazards, and intrusion
- Technical security services, including the use of passwords, encryption, and entity authentication
- Technical security mechanisms to guard against unauthorized access to data transmitted over a network

**Compliance and Enforcement**
A person who believes that a covered entity is not in compliance with HIPAA may file a complaint with the Secretary of the Department of Health and Human Services. The Secretary may investigate complaints and also may conduct reviews to determine compliance.

**Breaches**
If there is a breach of unsecured protected health information, the covered entity must provide notice to all affected individuals. A breach is defined as the "acquisition, access, use or disclosure” of protected health information in a manner that violates the Privacy Rule or the Security Rule, and which “compromises the security or privacy of the protected health
information.” A breach “poses a significant risk of financial, reputational, or other harm to the individual.”

**Violations**
A violation is an act that is contrary to the meaning or spirit of HIPAA and Appalachian State University guidelines to guarantee the confidentiality of protected health information. The following list outlines some, but not all, of the violations requiring sanctions:

**Level 1** violations can be considered careless errors. They include, but are not limited to:
- Accessing PHI that is not necessary for carrying out one’s responsibilities
- Misdirecting faxes or emails that contain PHI
- Discussing PHI in public areas or in areas where the public could overhear the conversation
- Copying or printing PHI without authorization
- Leaving a computer with PHI unattended
- Leaving a copy of PHI in a non-secure area
- Failing to cooperate with the institution’s designated privacy or security officials

**Level 2** violations can be considered willful actions. They include, but are not limited to:
- Unauthorized use or disclosure of PHI
- Discussing PHI with unauthorized healthcare professionals not directly associated with the case
- Asking another person to access or provide PHI without authorization
- Sharing computer information, such as passwords, that allows others to access PHI
- Having another person’s ID or password to access PHI
- Committing repeated Level 1 violations

**Level 3** violations can be considered malicious, flagrant, or egregious actions. They include, but are not limited to:
- Obtaining PHI under false pretenses
- Accessing or assisting someone else obtain PHI without an authorized reason
- Using PHI for commercial or personal purposes
- Discussing PHI with persons who are external to the clinic

**Sanctions**
When people associated with the Communication Disorders Clinic do not comply with the HIPAA policies and procedures, the Communication Disorders Clinic will use disciplinary action as defined in the policies and procedures of the University, the Student Code, and personnel manuals of the state of North Carolina. Sanctions for employees may include, but are not limited to, counseling, oral warning, written warning, suspension, or termination. Disclosures made as part of a “whistleblower” action will not be seen as violations.

For violations by students the penalties include, but are not limited to: counseling; reprimand; removal from the clinical practicum class, resulting in a failing grade; or total removal from the Department of Communication Sciences and Disorders.

**Reporting Violations**
All faculty, staff, and students are responsible for reporting suspected violations of privacy laws or privacy policies. All reports will be handled confidentially. Upon receiving a report, the Privacy Official will immediately conduct a thorough investigation and coordinate corrective measures, as
necessary. There will be no retribution or retaliation against anyone reporting a violation in good faith. Failure to report privacy violations will result in disciplinary action.

**Safeguards**
The Communication Disorders Clinic implemented procedures and made changes to provide the safeguards needed to protect the privacy and security of protected health information (PHI). The safeguards are contained in the Communication Disorders Clinic Policies and Procedures Manual, as well as this HIPAA Manual.

**Preemption of State Law**
In general, HIPAA preempts provision of state laws that are contrary to the HIPAA regulations. In states that have standards that substantially conform to or exceed these federal standards, or states that otherwise enforce the federal standards, state insurance regulators have primary enforcement authority for insurance carriers. For those states that do not have such standards, the Centers for Medicare and Medicaid Services "directly" enforces HIPAA and the related amendments.