SECURITY RULE

Security can be defined as "the state of being free from unacceptable risk". The risk concerns the following categories of losses:

- Confidentiality of information - the privacy of personal or corporate information
- Integrity of data - the accuracy of data
- Assets – including computer and peripheral equipment, communications equipment, computing and communications premises, power, water, environmental control, and communications utilities, supplies and data storage media, system computer programs and documentation, application computer programs and documentation and information
- Efficient and appropriate use - ensures that University IT resources are used for the purposes for which they were intended, in a manner that does not interfere with the rights of others
- System availability - concerned with the full functionality of a system (e.g. finance or payroll) and its components

The Security Rule has a compliance date of April 20, 2005. It outlines standards for the security of health information used by health plans, health care clearinghouses, and health care providers. The security standards apply to all individually identifiable health information that is in electronic form, whether it is being stored or transmitted. In order to administer their programs, the Department of Health and Human Services, other Federal and State agencies, private health plans, health care providers, and health care clearinghouses must assure their customers and clients that the confidentiality and privacy of health care information is secure. All healthcare providers, health plans, and clearinghouses that electronically store or transmit individual health information must comply.

Covered entities must ensure the confidentiality, integrity, and availability of all electronic protected health information. The information must be protected against any reasonably anticipated threats or hazards. The Department of Health and Human Services (DHHS) allows the covered entity to be flexible in its approach to reasonably and appropriately put into effect the standards and implementation specifications. DHHS provides this flexibility by stating whether the section of the Security Rule is “required” or “addressable.”

Information Security Definitions

Electronic Protected Health Information (EPHI) – individually identifiable health information, including demographic information, transmitted or maintained in electronic media, which is created or received by the entity.

Electronic storage media – includes memory devices in computers (hard drives) and any removable or transportable digital memory medium.

Transmission media – used to exchange information already in electronic storage media. It includes the internet, intranet (using internet technology to link information accessible to collaborating parties), networks, and the physical movement of removable or transportable electronic storage media.
**Device and Media Controls** – controls to provide accountability of the receipt and removal of hardware or software.

**Electronic Information System** – any electronic system or device that uses or contains (stores) confidential information including computers, laptops, PDAs, CD, floppy disks, etc.

**Encryption** – the process of disguising information as “cipher text” or data unintelligible to an unauthorized person.

**Information System** - an infrastructure for the storage, processing, transmission, input, and output of electronic information. Components may include computer hardware, software, and other manual or automated operational procedures.

**Security incident** - the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

**User** – anyone accessing an electronic device that stores, shares, receives, or exports confidential information.

**Work Station** – electronic system for accessing, modifying, or deleting electronic information including computers, key board, monitors, etc

---

**SECURITY STANDARDS**

Information and information systems at the Appalachian State University Communication Disorders Clinic are assets and are protected from accidental or unauthorized access, disclosure, modification, destruction, or denial through security controls. These security controls are sufficient to ensure confidentiality, reliability, integrity, audit capability, and availability of information.

The purpose of this policy is to establish a standardized, system-wide approach to managing the protection of information and information technology resources to support the business needs of the Clinic and the provision of quality care to the clients served through the Communication Disorders Clinic. The policies are designed to protect against any reasonably anticipated use or disclosure of information.

This policy applies to all workforce members as described in the Introduction of the HIPAA Manual. It covers all Clinic client information whether in hardcopy or electronic form and any systems which access, process, or have custody of client data. It applies to:

- All information, in any form and in any medium;
- All mainframe, network, internet, intranet, and personal computer environments;
- All creation, communication, distribution, storage, and disposal of information;
- All workforce members who have access to the Clinic’s information systems

The Appalachian State University Communication Disorders Clinic is a clinical training and business operation which employs eight (8) full-time clinical faculty members and five (5) part-time clinical faculty members. Additionally, five (5) fulltime clinical staff members employed through the Institute for Health and Human Services provide support services to the clients and faculty in the Communication Disorders Clinic. Fifty to fifty-five graduate students are trained annually, with roughly the same number admitted to the undergraduate program. Approximately
55+ clients attend treatment on a weekly basis with another 15-20 clients being seen for diagnostic evaluations weekly.

Information concerning EPHI generated on the computer networking system at the Clinic is on file at the Clinic.

**Administrative Safeguards**
Administrative safeguards include documented, formal policies, procedures, and practices to manage the selection and execution of security measures to protect data, and to manage the conduct of personnel in relation to the protection of data. These policies, procedures, and practices address items such as contingency planning in the case of a disaster in relation to information, information access control, sanctions for security policy violations, and employee training.


**Risk Analysis** (R) – conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI held by the covered entity.
Risk analysis means a systematic and analytical approach that identifies and assesses the risks to the confidentiality, integrity, or availability of a covered entity’s EPHI. Risk analysis considers all relevant losses that would be expected if specific security measures protecting EPHI are not in place. Relevant losses include losses caused by unauthorized use and disclosure of EPHI and loss of data integrity.

The Appalachian State University Communication Disorders Clinic conducts periodic accurate and thorough assessments of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of EPHI. These risk analyses will help form the foundation upon which security activities are built. Each analysis is documented in the HIPAA Manual and will be maintained for six years. Risk will be reassessed annually and updated as needed.

The procedure for updating the risk analysis is as follows:

1. The Clinic Security Official is responsible for the completion of and updating of Risk Analysis documents. At a minimum the risk analysis process includes the following:
   - Identification and prioritization of the threats to the Communication Disorders Clinic information systems containing EPHI.
   - Identification and prioritization of the vulnerabilities of the Communication Disorders Clinic information systems containing EPHI.
   - Identification and definition of security measures used to protect the confidentiality, integrity, and availability of the Communication Disorders Clinic information systems containing EPHI.
   - Identification of the likelihood that a given threat will exploit a specific vulnerability on a Communication Disorders Clinic information system containing EPHI.
   - Identification of the potential impacts to the confidentiality, integrity, and availability of Communication Disorders Clinic information systems containing EPHI if a given threat exploits a specific vulnerability.

2. Updates occur at least annually, when a new threat or vulnerability is identified or when new equipment or software is added. Any new equipment, information systems or computer systems that are installed will undergo the same review process. Such updates
must be used in conjunction with the Communication Disorders Clinic risk management process to identify, select, and implement security measures to protect the confidentiality, integrity, and availability of Communication Disorders Clinic information systems containing EPHI.

3. When possible the Communication Disorders Clinic risk analysis process should use both qualitative and quantitative data.

4. The Clinic Security Official is responsible for prioritizing the criticality of any EPHI that is identified as being at risk.

5. The Clinic Security Official, along with the University Security Official, makes decisions about security actions that become necessary.

6. If a suspicious activity is identified through routine security identification measures or by report, it is investigated and the results of such investigation are documented.

7. In addition to regular risk analysis, the Communication Disorders Clinic must conduct a risk analysis when environmental or operational changes occur, which significantly impact the confidentiality, integrity, or availability of specific information systems containing EPHI. Such changes include but are not limited to:

   - Significant security incidents to specific Communication Disorders Clinic information systems containing EPHI.
   - Significant new threats to specific Communication Disorders Clinic information systems containing EPHI.
   - Significant changes to the organizational or technical infrastructure of the Communication Disorders Clinic which affect specific Communication Disorders Clinic information systems containing EPHI.
   - Significant changes the Communication Disorders Clinic information security requirements or responsibilities which affect specific Communication Disorders Clinic information systems containing EPHI.

The Communication Disorders Clinic’s risk analysis process must be based on the following steps:

- **Inventory** – the Communication Disorders Clinic must conduct a regular inventory of its information systems containing EPHI and the security measures protecting those systems.

- **Threat identification** – The Communication Disorders Clinic must identify all potential threats to its information systems containing EPHI. Such threats may be natural, human, or environmental.

- **Vulnerability identification** – the Communication Disorders Clinic must identify all vulnerabilities on its information systems containing EPHI. This should be done by regularly reviewing vulnerability sources and performing security assessments.

- **Security control analysis** – The Communication Disorders Clinic must analyze the security measures that have been implemented or will be implemented to protect its information systems containing EPHI. This includes both preventive and detective controls.
- **Risk likelihood determination** – The Communication Disorders Clinic must assign ratings to specific risks that indicate the probability that vulnerability will be exploited by a particular threat. Three factors should be considered: 1) threat motivation and capability, 2) type of vulnerability, and 3) existence and effectiveness of current security controls.

- **Impact analysis** – The Communication Disorders Clinic must determine the impact to confidentiality, integrity, or availability that would result if a threat were to successfully exploit vulnerability on a Communication Disorders Clinic information system containing EPHI.

- **Risk determination** – The Communication Disorders Clinic must use the information obtained in the above steps to identify the level of risk to specific information systems containing EPHI. For each vulnerability and associated possible threat, the Communication Disorders Clinic must make a risk determination based on:
  - The likelihood a certain threat will attempt to exploit a specific vulnerability.
  - The level of impact should the threat successfully exploit the vulnerability.
  - The adequacy of planned or existing security controls.

**Risk Management (R)** – implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with the general requirements of the Security Rule. The Clinic must implement security measures and safeguards sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level. Selection and implementation of such security measures must be based on a formal, documented risk management process. The level, complexity, and cost of such security measures and safeguards must be commensurate with the risk classification. The Clinic must be safeguarded by normal best-practice security measures such as user accounts, passwords, and perimeter firewalls. (See Risk Analysis)

The selection and implementation of such security measures must be based on a formal, documented risk management process. At a minimum, the Communication Disorders Clinic’s risk management process must include the following:

- Assessment and prioritization of risks to the Communication Disorders Clinic information systems containing EPHI.
- Selection and implementation of reasonable, appropriate, and cost-effective security measures to manage, mitigate, or accept identified risks.
- Communication Disorders Clinic work force training and awareness on implemented security measures.
- Regular evaluation and revision, as necessary, of Communication Disorders Clinic’s security measures.

The Communication Disorders Clinic must manage risk on a continuous basis and all selected and implemented security measures must ensure the confidentiality, integrity, and availability of Communication Disorders Clinic information systems containing EPHI. Strategies for managing risk should be commensurate with the risks to such systems. One or more of the following methods may be used to manage risk:

- Risk acceptance
- Risk avoidance
- Risk limitation
- Risk transference
An analysis of all Communication Disorders Clinic and Appalachian State University information networks will be conducted on a periodic basis to document the threats and vulnerabilities to stored and transmitted information. In conjunction with Network Support Services (NSS) and the security official, the analysis will examine the types of threats - external and internal, electronic and non-electronic, natural and manmade - that affect the ability to manage the information resource. This group also will document the existing vulnerabilities within each entity which potentially expose the information within each entity which potentially expose the information resource to these threats. The periodic assessment will be implemented to reduce the impact of the threats.

The Communication Disorders Clinic’s risk management process must be based on the following steps:

- **Inventory** – the Communication Disorders Clinic must conduct a regular inventory of its information systems containing EPHI and the security measures protecting those systems.

- **Risk prioritization** – based on the risks defined by the Communication Disorders Clinic’s risk analysis, risks must be prioritized on a scale from high to low based on the potential impact to information systems containing EPHI and the probability of occurrence. When deciding what Communication Disorders Clinic resources should be allocated to identified risks, highest priority must be given to those risks with unacceptably high risk rankings.

- **Method selection** – The Communication Disorders Clinic must select the most appropriate security methods to minimize or eliminate identified risks to Communication Disorders Clinic information systems containing EPHI. Such selection must be based on the nature of a specific risk and the feasibility and effectiveness of a specific method.

- **Cost-benefit analysis** – The Communication Disorders Clinic must identify and define the costs and benefits of implementing or not implementing specific security methods.

- **Security method selection** – Based on its cost-benefit analysis, the Communication Disorders Clinic must determine the most appropriate, reasonable, and cost-effective security method(s) for reducing identified risks to Communication Disorders Clinic information systems containing EPHI.

- **Assignment of responsibility** – Communication Disorders Clinic workforce members who have the appropriate expertise must be identified and assigned responsibility for implementing selected security method(s).

- **Security method implementation** – Selected security method(s) must be correctly implemented.

- **Security method evaluation** – Selected security method(s) must be regularly evaluated and revised as necessary.

All Appalachian State University networks, systems, and applications are subject to the Appalachian State University Policy on the Use of Computers and Data Communications (see HIPAA Manual). Networks, systems, and applications that may send, receive, store, or access EPHI must also comply with the HIPAA Security Policies.

**Sanction Policy (R)** – apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity. The Communication Disorders Clinic workforce must comply with all applicable Communication Disorders Clinic
security policies and procedures. When people associated with the Clinic do not comply with the HIPAA policies and procedures, the 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, or total removal from the clinical practicum class, resulting in a failing grade.

All faculty, staff, and students are responsible for reporting suspected violations of security laws or security policies. All reports will be handled confidentially. Upon receiving a report, the Security 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 security violations will result in disciplinary action.

**Information System Activity Review (R)** – implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports. The Communication Disorders Clinic must regularly review records of activity on information systems containing EPHI. Appropriate hardware, software, or procedural auditing mechanism must be implemented in Communication Disorders Clinic information systems that contain or use EPHI. The entity needs to document what and how often EPHI records are reviewed to ensure there has been no security incidents that warrant attention. Records of activity may include but are not limited to:

- Audit logs
- Access reports
- Security incident tracking reports

Such reviews must be accomplished via a formal documented process. At a minimum, the process must include:

- Definition of which workforce members will review records of activity
- Definition of which activity is significant
- Definition of which activity records need to be archived
- Procedures defining how significant activity will be identified and reported

The level and type of auditing mechanisms that must be implemented on Communication Disorders Clinic information systems that contain or use EPHI must be determined by the risk analysis process. Auditable events can include but are not limited to:

- Access of sensitive client data
- Use of audit software programs or utilities
- Use of a privileged account
- Information start-up or stop
- Failed authentication attempts
- Security incidents

Whenever possible, Communication Disorders Clinic workforce members should not monitor or review activity related to their own user account. Further information concerning Appalachian State University Policy is included in the HIPAA Manual.
Standard: Assigned Security Responsibility (R) – identify the security official for the development of the policies and procedures required by this subpart for the entity. The Clinic created a role of security official who is responsible for development, implementation, and maintenance of HIPAA security policies and procedures for the Clinic. The role is filled by the Director of the Clinic. The Clinical Issues Committee serves as the Security Oversight Committee.

The Information Security Official for the University oversees all activities related to HIPAA security regulations and security policies. This individual is responsible for the development and implementation of the policies and procedures required by the Security Rule. The University Security Official is Michael Bennett (262-6068). His primary responsibility is to the Communication Disorders Clinic.

The responsibilities of the Information Security Official are to work with the covered entities to develop and implement security policies, procedures and controls. Working together with the Clinic Director, duties would include:

- Ensuring that Communication Disorders Clinic information systems comply with all applicable federal, state, and local laws and regulations.
- Ensuring that no Communication Disorders Clinic information system compromises the confidentiality, integrity, or availability of any other Communication Disorders Clinic or Appalachian State University information systems.
- Developing, documenting, and ensuring dissemination of appropriate security policies, procedures, and standards for the users and administrators of Communication Disorders Clinic information systems and the data contained within them.
- Ensuring that newly acquired Communication Disorders Clinic information systems have features that support required or addressable security implementation specifications.
- Coordinating the selection, implementation, and administration of significant Communication Disorders Clinic security controls.
- Conducting periodic risk analysis of Communication Disorders Clinic information systems and security processes.
- Developing and implementing an effective risk management program.
- Regularly monitoring and evaluating threats and risks to Communication Disorders Clinic information systems.
- Developing and monitoring audit records of Communication Disorders Clinic information systems to identify inappropriate activity.
- Maintaining an inventory of all Communication Disorders Clinic information systems that contain EPHI.
- Advising systems, application, and development owners in the implementation of security controls for information on systems, from the point of design, through testing and product implementation.
- Creating an effective security incident response policy and related procedures.
- Ensuring adequate physical security controls exist to protect Communication Disorders Clinic EPHI.
- Evaluating new security technologies that may be appropriate for protecting Communication Disorders Clinic information systems.
- Reporting regularly to the Clinical Issues Committee.

Appalachian State University, along with the state of North Carolina, is the owner of all information generated in the Communication Disorders Clinic. As such Appalachian State University is responsible for:

- Ensuring appropriate procedures are in effect to protect the integrity, confidentiality, and availability of the information used and created within the covered entity.
Knowing the information for which it holds the responsibility.
Authorizing access and assigning custodianship.
Following existing approval processes within the organization for the selection, purchase, implementation, and budgeting of a computer system or software to manage information.

The Communication Disorders Clinic is the custodian of the information. As such the clinic is responsible for the processing and storage of the information. Responsibilities include:

- Administering access to information
- Providing and recommending physical and procedural safeguards
- Evaluating the cost effectiveness of controls
- Maintaining information security policies, procedures, and standards
- Promoting employee education and awareness
- Identifying and responding to security incidents and initiating appropriate actions when problems are identified.

The Communication Disorders Clinic management supervises users of the information as defined below. Management is responsible for overseeing employees' use of information, including

- Promptly informing the appropriate parties of employee termination and transfers, in accordance with local entity termination procedures
- Providing employees with the opportunity for training needed to properly use the computer systems
- Initiating corrective actions when problems are identified
- Reviewing and approving all requests for access authorization
- Initiating security change requests to keep employee security record current with their position and job functions
- Initiating corrective actions when breaches or problems are identified

The user is a person who has been authorized to read, enter, or update information. A user of information is expected to:

- Comply with HIPAA Security Policies and Standards and with all established controls
- Access information only in support of their authorized job responsibilities
- Keep personal authentication devices (e.g. passwords) confidential

**Standard: Workforce Security** - *implement policies and procedures to ensure that all members of its workforce have appropriate access to EPHI, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to EPHI. Workforce security includes information concerning authorization and/or supervision, workforce clearance procedures, and termination procedures. The Communication Disorders Clinic must prevent unauthorized access to information systems. Only properly authorized workforce members must be provided this access. The type and extent of access authorized to Communication Disorders Clinic information systems containing EPHI must be based on the current risk analysis. Access to Communication Disorders Clinic information systems containing EPHI must be granted only to properly trained Communication Disorders Clinic workforce members who have a need for EPHI in order to accomplish a legitimate task.*
All workforce members receive clearance to access PHI through the HIPAA privacy and security training. Workforce members must have a legitimate need for specific information in order to accomplish job responsibilities. All such access must be defined and documented. All workforce members are responsible for alerting the Security Official to situations that might raise concern regarding a threat to security. The Clinic Security Official makes a determination as to any special security measures that should be taken.

- The Communication Disorders Clinic must protect the confidentiality, integrity, and availability of its information systems containing EPHI by preventing unauthorized access while ensuring that properly authorized workforce member access is allowed.
- The type and extent of access to information systems containing EPHI must be based on risk analysis.
- Communication Disorders Clinic workforce members must not attempt to gain access to information for which they have not been given proper authorization.

**Implementation: Authorization and/or Supervision (A)** – implement procedures for the authorization and/or supervision of workforce members who work with EPHI or in locations where it might be accessed. The Communication Disorders Clinic must ensure that all workforce members who can access Communication Disorders Clinic information systems containing EPHI are appropriately authorized and supervised. The type and extent of access granted to Communication Disorders Clinic information systems containing EPHI must be based on risk analysis. Access to Communication Disorders Clinic information systems containing EPHI must be authorized only for Communication Disorders Clinic workforce members having a need for specific information in order to accomplish their respective job responsibilities.

All faculty, staff, and students are responsible for being aware of, and complying with, the Security Regulations and the Security Policies and Procedures. All faculty, staff, and students are required to complete a HIPAA Training Course annually with documentation to their clinic file. The Director of the Clinic along with the Clinical Issues Committee will determine what access will be granted to authorized students and employees. Anyone who is not authorized will be supervised by the designated person authorized by the Security Official before gaining temporary access.

EPHI (client reports primarily) is stored on the networking system at the Clinic. Information concerning this system is on file in the Clinic.

**Implementation: Workforce Clearance Procedure (A)** – implement procedures to determine that the access of a workforce member to EPHI is appropriate. The need for and extent of a screening process is normally based on an assessment of risk, cost, benefit, and feasibility as well as other protective measures in place. For the Communication Disorders Clinic certain client information is kept on only one or two computers with limited access. This would include, but is not limited to, the client database, client hearing aid information, and payment history. Other EPHI is kept at the discretion of the faculty and staff with appropriate training modules concerning the information in effect. All Communication Disorders Clinic workforce members who access Communication Disorders Clinic information systems containing EPHI must sign a confidentiality agreement.
The background of all Communication Disorders Clinic workforce members must be adequately reviewed during the hiring process. Verification checks must be made, as appropriate. Verification checks include, but are not limited to:

- Character references
- Confirmation of claimed academic and professional qualifications
- Professional license validation
- Criminal background check

All workforce members receive clearance to access PHI through HIPAA privacy and security training. All employees are required to participate in privacy and security awareness training with documentation of such participation immediately upon their hire. All workforce members sign an acknowledgement training form, which is maintained in their personnel file or a central HIPAA Privacy/Security Notebook. Graduate students also sign a confidentiality statement prior to beginning clinical practicum regarding the protection of PHI at the Clinic. Personnel will not be allowed access until all training is completed and documented.

**Implementation: Termination Procedures (A)** – Implement procedures for terminating access to EPHI when the employment of a workforce member ends or as required by determination made as specified in paragraph (a)(3)(ii)(B) of this section. When the employment of Communication Disorders Clinic workforce members ends, their information systems privileges, both internal and remote, must be disabled or remove by the time of departure. In the Communication Disorders Clinic the steps taken to terminate access to information include, but are not limited to, turning in keys to the Clinic, deactivation of user identification numbers and passwords, and removal from access lists. The keys for the College of Health Sciences and Appalachian State University cannot be duplicated and a master list of all disseminated keys is maintained in the Dean’s Office as well as in the Clinic Director’s Office.

In the event an employee is terminated or resigns the following procedures should be followed to ensure the privacy and security of PHI at the Clinic:

- All keys to the Clinic are returned;
- Identification badge (nametag) is returned;
- All equipment/software, desk, and working premises is inventoried;
- Network administrator notified for revoking electronic access to systems or records containing protected health information;
- If needed, notify officers of the ASU Police for revoking physical access to records containing protected health information.

**Standard: Information Access Management** - Implement policies and procedures for authorizing access to EPHI.

**Implementation: Isolating Health Care Clearinghouse Function** (R) – those components that are designated as health care components must comply with the security standards and protect against unauthorized access with respect to the other components of the larger entity in the same way as they must deal with separate entities.

The Appalachian State University Communication Disorders Clinic employs the services of a clearinghouse for electronic claims submission. VantageMed Corporation serves as the intermediary between the Clinic and third-party payers. The clearinghouse facilitates the electronic exchange of information between the two entities. The clearinghouse function is maintained on the computers in the Clinic Office and only three clinic staff member and the Clinic Director have access to the system.
Implementation: Access Authorization (A) – *implement policies and procedures for granting access to EPHI*, for example, through access to a workstation, transaction, program, process, or other mechanism. Access authorization embraces the implementation of policies and procedures that grant access to electronic PHI. For the Communication Disorders Clinic certain PHI is accessed only by those persons authorized by the Director of the Communication Disorders Clinic. This would include, but not limited to, client charts, the client database, client hearing aid and voice evaluation information, and payment history. Other electronic PHI is kept at the discretion of the faculty and staff as authorized by the Director of the Communication Disorders Clinic.

Any individual attempting to or requesting someone else to circumvent security or administrative access controls for information systems is in violation of this policy. Furthermore, unauthorized use, alteration, destruction or disclosure of systems identification, passwords, or confidential information will be dealt with according to policies and procedures developed for University and state employees.

Implementation: Access Establishment and Modification (A) – *implement policies and procedures that, based upon the entity’s access authorization policies, establish, document, review, and modify a user’s right of access to a workstation, transaction, program, or process.* The Communication Disorders Clinic must have a formal documented process for establishing, documenting, reviewing, and modifying access to Communication Disorders Clinic information systems containing EPHI. EPHI (client reports primarily) is stored on the networking system at the Clinic.

Client records, entire or partial, are never to be removed or transmitted in an unauthorized way, from the Clinic for any reason by the workforce personnel. Clinic faculty disclosing PHI to another facility for treatment purposes must follow the procedures for such as outlined in the Privacy Section of this Manual.

A client's record is never to be altered or manipulated in any way by a graduate student once it is approved by the appropriate clinical faculty workforce member. Once the information has been processed and filed in the client chart (thus becoming PHI) any errors noted on diagnostic or other clinical reports are to be modified by hand in black ink with the initials of the workforce member noted next to the change.

Protected Health Information is not to be transmitted via electronic mail by any of the workforce members, unless following the steps as outlined in the Email Policy as outlined in the HIPAA Manual.

Electronic protected health information (ePHI) generated on the computer networking system at the Clinic is transmitted from computer to computer over local lines to a main cabletron switch provided by ASU Computer Services. Computer to computer traffic remains local and in the building. Billing information is transmitted outside of the building to a server in the Reich College of Education. The information is transmitted over the ASU network back to campus to another main cabletron switch in Computer Services Center with tipping point services to monitor prior and identify malicious traffic. From Computer Services, it runs over the local ASU network to the server building in Raley Hall Computer Center. The Center is capable of providing/implementing security measures to the physical plant as well as to all hardware and software. The billing information has an encrypted system that it uses.

Standard: Security Awareness and Training – *implement a security awareness and training program for all members of the workforce (including management).* Workforce members will receive training in security policies and procedures for the Clinic upon their hire. Students will
receive training before beginning clinical practicum. The goals of the training program are to describe the policies and procedures related to the security of:

- Workstations
- Password management
- E-mails
- Client charts
- Use of the networking system
- Physical Security (buildings)

Security training may be provided in several formats. Training is documented for all faculty, staff and students and maintained in their files in the Clinic Office.

**Security Reminders (A) – periodic security updates.** The Communication Disorders Clinic must make certain that all of its workforce, including those who work remotely, are regularly reminded of information security risks and how to follow Communication Disorders Clinic security policies. Additionally, workforce members must be provided with information about Communication Disorders Clinic security policies and how to use Communication Disorders Clinic information systems in ways that minimize possible risks.

On a regular basis the Communication Disorders Clinic must provide all of its workforce members with information and reminders on topics including, but not limited to:

- Communication Disorders Clinic information security policies
- Significant Communication Disorders Clinic information security controls and processes
- Significant risks to Communication Disorders Clinic information systems and data
- Security best practices (e.g. how to choose a good password, how to report a security incident)
- Communication Disorders Clinic information security legal and business responsibilities

Security updates are sent to the faculty, staff and students via email on an as needed basis. Such information reminders are provided at the Communication Disorders Clinic or via the list serve email. All faculty, staff, and students must participate in annual HIPAA Workshops, which include security updates. Security checks are conducted at the Clinic by administrative staff workforce members. Workstations and facility security are the primary focus of the monthly reviews. Notification regarding non-compliance with the Clinic's security policies and procedures will be provided in writing. Mitigation and sanctions are also documented.

In addition to providing regular information security awareness, Communication Disorders Clinic must provide security information and awareness to all of its workforce when any of the following events occur:

- Significant revisions to Communication Disorders Clinic’s information security policies or procedures.
- Significant new information security controls are implemented at the Communication Disorders Clinic.
- Substantial changes are made to significant Communication Disorders Clinic information security controls.
- Significant changes occur to Communication Disorders Clinic’s information security legal or business responsibilities.
- Significant new threats or risks arise against Communication Disorders Clinic information systems or data.

**Protection from Malicious Software (A) – procedures for guarding against, detecting, and reporting malicious software.** The Communication Disorders Clinic must regularly train and remind its workforce members about its process for guarding against, detecting, and reporting malicious software that poses a risk to its information systems.
Appalachian State University has processes in place to detect and prevent malicious software, particularly viruses, worms, and malicious code. The entire university receives notices when a problem is detected. All computers used by faculty and students have automatic installation and regular updating of anti-virus software on all University information systems. VirusScan is updated at least every three hours. Information Technology Services conducts an examination of data on electronic media and data received over networks to ensure that it does not contain malicious software. Workforce members are not to open email or attachments from an unknown or unrecognizable source. Virus advisories are routinely distributed by the Information Technology Services. The antivirus programs are never to be disabled on any computer used in the Clinic.

The Information Technology Services (ITS) provides technical computer networking infrastructure support to authorized users for access to the university communications backbone. This includes the design, installation, monitoring and support of specialized communications equipment attached to the campus backbone as well as access to external networks. Network security, network user registration and network configuration functions are provided and coordinated by ITS. ITS supports and configures all switches and routers that make up the university data network backbone and coordinates its activities closely with other campus units involved with premise wiring, network planning and support.

The university has policies regarding all electronic mail attachments and data downloads for malicious software before use on information systems and there are procedures for members of the workforce to report suspected or known malicious software.

There is an appropriate disaster recovery plan for recovering from malicious software attacks. Procedures to verify that all information relating to malicious software is accurate and informative.

Workforce members are reminded to not modify web browser security settings without appropriate authorization and they cannot install unauthorized software on university information systems. Specific information concerning university policies in found in the Appalachian State University Computer Use Policy.

**Log-In Monitoring (A)** – procedures for monitoring log-in attempts and reporting discrepancies. The Communication Disorders Clinic must provide regular training and awareness to its workforce members about its procedures for monitoring log-in attempts and reporting discrepancies. Information concerning specific log-in information for faculty and students is on file in the Clinic. All personnel are trained concerning proper log-in procedures.

User login identifications, passwords or e-mail accounts are never to be transferred to another individual. New accounts are requested by a workforce member/administrative assistant at the Clinic following approval by the Clinic Director. ITS assigns passwords.

**Password Management (A)** – procedures for creating, changing, and safeguarding passwords. The Communication Disorders Clinic must regularly train and remind its workforce about the process for appropriately creating, changing, and safeguarding passwords. At a minimum Communication Disorders Clinic’s password management system must:

- Require the use of individual passwords to maintain accountability.
- Where appropriate, allow workforce members to select and change their own passwords.
- Require unique passwords that meet the standards defined by Appalachian State University policies.
- Require regular password changes.
- Not display passwords in clear text when they are being input into an application.
- Require that passwords be given to users in a secure manner.
- Require the changing of default vendor passwords following installation of software.

Passwords must be a minimum of 6 characters (or the maximum allowed for those applications that do not support a 6-character password). When an initial password is created for a new user, or reset, the individual must change his/her password at the next log-in. Passwords are changed every 90 days. Users are responsible to ensure that their passwords are changed every 90 days on systems which access patient or sensitive business information, as well as applications that do not support automatic password change notification. Passwords are to be a combination of alphanumeric characters. They should not be easily guessed. Generic user passwords are not permitted at the computer application level. User IDs and passwords are not to be shared.

Password Administration - Failed login attempts will be recorded and reviewed by the Security Official for follow up action. Users are locked out of the system for 30 minutes after three failed login attempts. During that time the account lockout counter is reset and the workforce member may login after that time. Appropriate access privileges are reviewed prior to granting access based upon several factors including job title and function (role-based access) or the individual, (user-based access). Accounts of graduating students or terminated employees are deleted immediately upon graduation or termination of job.

User passwords or e-mail accounts are not to be transferred to another individual. New accounts are obtained by calling ITS. Approval by the Security Official is required before any account can be created.

As a pre-requisite to resetting a User’s password, the User identity must be verified in person, prior to resetting the password. **Resetting of passwords may not be requested by e-mail.** Managers are cautioned that one popular method of breaking into a computer system is by those who falsely claim another’s identity. Verification may be accomplished by:

> Presenting in person, with the workforce members ID badge to the administrator, or presenting in person to the director or administrative staff, or by voice to a manager who will recognize the user’s voice and the manager in turn will authorize the system administrator, analyst or operator via email to reset the User’s password. It is the administrative staff person’s responsibility to require the User to present in person, if they are unsure of the voice identification.

> By voice to an administrative staff person, operator or analyst who has access to a personal identification code, password, maiden name, etc.

Misuse and Unauthorized Access - The misuse of or sharing of passwords may lead to disciplinary action as outlined in the **Security Management Process** section of this manual.

**Standard: Security Incident Procedures** - implement policies and procedures to address security incidents.

**Implementation: Response and Reporting** (R) – identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity; and document security incidents and their outcomes. The Communication Disorders Clinic must be able to effectively detect and respond to security incidents in order to protect the confidentiality, integrity, and availability of its information systems. All breaches of security are to be reported either verbally or in writing to the Security Official and documented in the HIPAA Manual. The Security Official in turn notifies all
appropriate individual(s) in writing of the security violation. Policies will be reviewed to determine if better, more appropriate procedures may have prevented the security breach. Mitigation and sanctions will be documented.

All individuals under contract with the Management Company to provide maintenance at the Clinic are required to report in at the main desk. A "Visitor" badge is issued if appropriate self-identification is not visible (e.g. a uniform with company name, etc.).

The Security Official determines the necessary steps to mitigate the harmful effects of any security incident and documents the mitigation. The Security Official documents the security incident, the outcome of the investigation, and the response to the incident.

Workforce members are trained to understand their responsibility for recognizing and reporting a security incident in accordance with the protocol for reporting security incidents.

**Standard: Contingency Plan** - *establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain EPHI.* The Communication Disorders Clinic must prepare for and be able to effectively respond to emergencies or disasters in order to protect the confidentiality, integrity, and availability of its information systems.

**Implementation: Data Back-up Plan (R)** – *establish and implement procedures to create and maintain retrievable exact copies of EPHI.* The electronic PHI on Communication Disorders Clinic information systems and electronic media must be regularly backed up and securely stored. Back-up and restoration procedures must be regularly tested. All data on the RCOE server, including Therapist Helper information is transferred to a back-up tape every day. Back-up is performed on all high and medium risk files. The back-up tapes are stored off-campus. In the event of an emergency all electronic information is retrievable and the Clinic operations can proceed.

**Implementation: Disaster Recovery Plan (R)** – *establish (and implement as needed) procedures to restore any loss of data.* The Communication Disorders Clinic must create and document a disaster recovery plan to recover its information systems if impacted by a disaster. Communication Disorders Clinic personnel must receive regular training and awareness on the disaster recovery plan. It entails the what, who, and how to restore data after an emergency. In the event of a natural disaster, the Clinic first implements the appropriate disaster plan outlined by the University in the Emergency Response Plan. All appropriate Communication Disorders Clinic workforce members must have a current copy of the plan and copies of the plan must be kept off-site.

**Implementation: Emergency Mode Operation Plan (R)** – *establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of EPHI while operating in emergency mode.* The Communication Disorders Clinic must have a formal, documented emergency mode operation plan to enable the continuation of crucial business processes that protect the security of its information systems containing EPHI during and immediately after a crisis situation. The ability to maintain client services and to continue clinical training of graduate students in the event of a natural disaster or other emergency is paramount to the mission of our organization. The ability to provide services and training without technology is highly feasible. Billing and claims processing without computer support is somewhat more difficult but is possible.

The Clinic implements the following procedures once the physical facility has been secured and clearance to begin operations is given:
• Assess damage to the inventory of supplies, tests, materials, and software programs; determine critical needs in order to continue programming and training. Re-order necessary supplies. Personnel responsible: Clinic Director, Clinical Faculty.

• Contact computer support for backup files. Personnel responsible: Billing Specialist.

• Notify all workforce members and students either by phone or by the Clinic email system when services will resume. Personnel responsible: Administrative Assistants.

• Re-assign, as necessary, client services to one of several off-site facilities. Personnel responsible: Clinic Director, Administrative Assistants

• Notify clients of re-assignments. Personnel responsible: Administrative Assistants

• Suspend billing and claims processing until clearance is given from computer support services; process claims by hand if approved by insurance companies, or on a computer in another location. Personnel responsible: Billing Specialist.

• Schedule appointments by hand; maintain a hand-written schedule to be transferred to the computer database once the system is restored.

The following preventive measures are implemented to reduce the risk of a lengthy recovery period and/or disruption of critical services, including billing:

• Copies of Clinic inventory (supplies, tests, materials, and software programs) and clinical faculty schedules are stored off-site.

• Back-up copies of past client records are stored off-site. The accessibility of all CD's containing past client records will be checked annually.

• Retrieval of back-up copies of client records is available on the server from the Computer Support staff.

**Implementation: Testing and Revision Plan** (A) – implement procedures for periodic testing and revision of contingency plans. The Communication Disorders Clinic must conduct regular testing of its contingency plan to ensure that it is up to date and effective. This is to test if all the above plans actually work. Routine review of the Clinic's evacuation plans in case of emergencies other than fire (e.g. severe weather threats, tornadoes, etc.) is done on an annual basis. Workforce members sign acknowledgement statements upon completion of annual evacuation training. The results of testing must be formally documented and presented to appropriate management.

As appropriate, the following types of tests can be on Communication Disorders Clinic contingency plan:

• **Paper test**: A detailed walk-through of the plan that typically includes tasks such as validating the vendor and notification lists and end user procedures.

• **Limited scope test**: A test of one or more components of the disaster recovery plan. Typical test tasks include using backup tapes to restore selected information systems at a remote recovery facility or on test machines within the Communication Disorders Clinic; and testing communications between the Clinic and its alternate/recovery facility or facilities.

• **Simulated full-scale disaster**: A complete test of disaster recovery plan. Such testing typically requires executive management support and extensive planning.
Personnel from the Office and Safety and Workman’s Compensation conduct live fire drills on a yearly basis. Documentation of all fire drills is maintained by the Office of Safety and Workman’s Compensation.

The Clinic’s Emergency Operation Plan is reviewed annually by the Security Official. The University Security Official assures that ITS conducts an annual audit of the computer system and procedures.

**Implementation: Applications and Data Criticality Analysis (A)** – *assess the relative criticality of specific applications and data in support of other contingency plan components.* The Communication Disorders Clinic must have a formal process for defining and identifying the criticality of its information systems and the data contained within them. This determines what applications and data need to be available for emergency mode operations to provide the proper security protection of the electronic PHI. The Clinic does not maintain computerized client charts on the networking system. Electronic PHI is converted to paper. Client charts containing PHI in paper form are maintained on all active patients and inactive patients up to three years. Paper copies of client charts (6 years or older) are maintained in a secured area in University Archives for an additional 12 years or until a child reaches 24 years of age as required by North Carolina law.

**Standard: Evaluation (R)** – *perform a periodic technical and non-technical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of EPHI, that establishes the extent to which an entity’s security policies and procedures meet the requirements of this subpart.* It establishes the extent to which security policies and procedures meet the requirement of this rule. The following procedures are used to conduct surveys of all computer and information systems to determine where EPHI is stored, how it is transmitted, and which Users currently have access:

- Internal evaluations are conducted on an annual basis
- Internal evaluation are conducted by the designated workforce members and/or the Clinic Security Official
- Checklists, questionnaires, and interviews are utilized for documentation purposes
- Review of login data is part of this annual evaluation
- Evaluations are done any time new technology concerning electronic PHI is adopted
- Key findings and recommendations are documented in a report

Any member of the Clinical Issues Committee or any other person associated with the Department of Communication Sciences and Disorders may suggest changes to the Security Policies or Procedures by submitting such suggestion for consideration.

The Clinical Issues Committee will review any suggested Security Policy or Procedure change and make preliminary recommendation. If the Clinical Issues Committee recommends a change, it will be communicated to the Security Official for the University.

In the event that one or more of the following events occur, the policy evaluation process will be triggered

- Changes in the HIPAA Security or Privacy Regulations
- New federal, state, or local laws or regulations affecting the privacy or security of PHI
Changes in technology, environmental processes, or business processes that may affect HIPAA Policies
A serious security violation, breach, or other security incident occurs

Any training for the Department of Communication Sciences and Disorders faculty, staff, and students will reflect any new policies established.

**Standard: Business Associate Contracts and Other Arrangements** (R) – a covered entity may permit a business associate to create, receive, maintain, or transmit EPHI on the covered entity’s behalf only if the covered entity obtains satisfactory assurances that the business associate will appropriately safeguard the information.

A covered entity that violates the satisfactory assurances it provided as a business associate of another covered entity will be in noncompliance with the standards, implementation specifications, and requirements. The Communication Disorders Clinic may permit a business associate to create, receive, maintain, or transmit EPHI on its behalf only if there is a written agreement between the Clinic and the business associate that provides assurances that the business associate will appropriately safeguard the information. If a breach occurs with the Business Associate, then the Business Associate must notify the Communication Disorders Clinic and rectify the breach.

**Implementation: Written contract or other arrangement** (R) - document the satisfactory assurances required this section through a written contract or other arrangement with the business associate that meets the applicable requirement. A business associate may create, receive, maintain, or transmit electronic PHI on the behalf of the covered entity. A written contract will ensure safeguards.

The Clinic maintains Business Associate contracts with all individuals, companies, etc. that perform a business associate function. All contracts are reviewed annually by the Clinic Director and Office Manager in order to document security compliance. Possible violations of security procedures are documented in the HIPAA Manual and forwarded on to legal counsel for a final determination on the contract status.

**Physical Safeguards**

Physical safeguards include the protection of physical computer systems and related buildings and equipment from intrusion, fire, and other natural and environmental hazards. They also cover the use of locks, keys, and administrative measures used to control access to computer systems and facilities.

The category of physical safeguards is focused on preventing unauthorized individuals from gaining access to electronic information. The five areas of physical safeguards include:

2. Media Controls – setting up formal procedures for controlling and tracking the handling of hardware and software, and for data backup, storage, and disposal.
3. Physical Access Controls – developing a physical security plan, setting up disaster recovery, emergency modes, and other access and handling controls.
4. Work Station Use – policies and procedures to prevent unauthorized access to protected information on work stations and terminals.
5. Security Awareness Training – awareness training for all employees and others with physical access to protected health information.
**Standard: Facility Access Controls** – *implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.* The Communication Disorders Clinic must appropriately limit physical access to the information systems contained within its facilities while ensuring that properly authorized workforce members can physically access such systems. Communication Disorders Clinic information systems containing EPHI must be physically located in such a manner as to minimize the risk that unauthorized persons can gain access to them. The level of protection must be commensurate with that of identified risks.

**Implementation: Contingency Operations** (A) – *establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.* The Communication Disorders Clinic must have formal, documented procedures for allowing designated individuals to enter its facilities to take necessary actions as defined in the Disaster Recovery and Emergency Mode Operations Plans.

The following preventive measures are implemented to reduce the risk of a lengthy recovery period and/or disruption of critical services, including billing:

- Copies of Clinic inventory (supplies, tests, materials, and software programs) and clinical faculty schedules are stored off-site.

- Back-up copies of past client records are stored off-site. The accessibility of all CD's containing past client records will be checked annually.
  - Retrieval of back-up copies of client records is available on the server from the Computer Support staff.
  - Since most client information is in paper-form, restoration would include replicating as much of an actual client chart as possible.

**Implementation: Facility Security Plan** (A) – *implement policies and procedures to safeguard the facility and equipment therein from unauthorized physical access, tampering, and theft.* The Communication Disorders Clinic must have a facility security plan that details how it will protect its facilities and the equipment therein, from unauthorized access, tampering, or theft of its EPHI.

The primary threat to the physical facility is theft followed by fire and natural disasters to include flood, tornados, and hurricanes. Security measures include maintaining locked doors in order to prevent the public easy access to the buildings where Clinic personnel are not available to monitor the area. Daily closing procedures by the administrative staff require that all office and therapy doors as well as the file room and access doorways leading to exits be locked. Workforce members who remain in the building after closing are responsible for ensuring that the exit doors used are secured. A key check-out system is in place.

All workforce members (graduate students, faculty, and staff) are to wear identification nametags at all times while at the Clinic. Visitors to the Clinic also check in at the front desk and are issued a “visitor” nametag. All maintenance personnel are required to check in at the main desk. Authentication of identification by the administrative staff is required whenever proper identification is not demonstrated.

**The Student Preparation Room** is accessible to students enrolled in the Department of Communication Sciences and Disorders, as well as students from other various clinics in the Institute for Health and Human Services. Students viewing protected health information and working on computers should be mindful of others in the room. Other people entering the room without permission are to be reported to the Clinic Director.
Implementation: Access Control and Validation Procedures (A) – Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision. Although all clinical staff and faculty have keys for the pertinent clinic areas, students do not receive keys for the Clinic. The Clinic Director has been issued a key for the Clinic Office. An annual audit of keys for the Clinic is conducted by staff members. University keys cannot be duplicated.

Maintenance personnel entering the Clinic check in at the main desk before proceeding to the designated work area. Visitors are escorted by a workforce member to their destination. Validation of individuals entering the building without visible identification is required.

Implementation: Maintenance Records (A) – Implement policies and procedures to document repairs and modifications to the physical components of a facility, which are related to security (for example, hardware, walls, doors, and locks). The Communication Disorders Clinic must document all repairs and modifications to the physical components of its facilities that are related to the security of its EPHI. All repair work to the Clinic is done by workforce members from the Physical Plant at Appalachian State University. A log of repair work is maintained in the Clinic Office. All calibration and equipment repair is maintained with the particular piece of equipment.

Standard: Workstation Use (R) – Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access EPHI. The Communication Disorders Clinic workstations must be used only for authorized purposes. Workforce members must not use Communication Disorders Clinic workstations to engage in any activity that is either illegal under local, state, federal, or international law or is in violation of Appalachian State University. Access to Communication Disorders Clinic workstations with EPHI must be controlled and authenticated. It includes logging off before leaving a workstation unattended, not sharing passwords, and not letting others use a workstation.

Workstation use is reserved for those individuals who are designated workforce members of the covered entity. Furthermore, workstations are restricted for use by those members assigned to the workstation.

Computer terminals in the office are positioned in such a way that they cannot be viewed by unauthorized persons. Students are warned to position screens where they cannot be viewed when the student is typing client reports. Students cannot save reports on a hard drive on any of the computers in the Student Work Room.

Standard: Workstation Security (R) – Implement physical safeguards for all workstations that access EPHI, to restrict access to authorized users. Workstation members who, and workstation and other computer systems used to send, receive, store, and access electronic PHI must comply with the Appalachian State University Computer Use Policy. Workforce members that use Appalachian State University information systems and workstation assets should have no expectation of privacy. To appropriately manage its information systems and enforce appropriate security measures, Appalachian State University may log, review, or monitor all data stored or transmitted on its information system assets (implement physical safeguards for all workstations that access electronic PHI, in order to restrict access to authorized users).

Confidential electronic health system information, either stored in or accessed through the computers or a network system, is to be secure at all times. Access to computer systems is restricted to those authorized for such access, and who have been issued appropriate unique
User IDs and passwords. Generic User IDs are not permitted at the computer application level. User IDs and Passwords are not to be shared. Screen savers with passwords should be used for desktop computers and are activated after no more than 1 minute of inactivity. Terminals in high traffic or public areas or with access to confidential information are to employ automatic workstation lock down after fifteen (15) minutes of inactivity. This potentially improves the integrity of the system and discourages access by others under one’s password, when an individual has stepped away from their computer while still logged into a system. It is occasionally necessary to disable screen saver passwords, for example, when PC Tech Support is expected for service of the computer.

Client records and therapy performance data stored on any laptop computer are password protected.

**Standard: Device and Media Controls** - implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of a facility, and the movement of these items within the facility. EPHI on Communication Disorders Clinic information systems and electronic media must be protected, accounted for, properly stored, backed up and disposed of in accordance with specific procedures. These controls must be in place for hardware and electronic media into, out of, and within the facility.

**Implementation: Disposal** (R) – implement policies and procedures to address the final disposition of EPHI, and/or the hardware or electronic media on which IT is stored. All Communication Disorders Clinic information systems and electronic media containing EPHI that is no longer required must be disposed of in a secure manner. Disposal of electronic media containing PHI must be tracked and logged. When computer media containing EPHI is to be disposed of or reused, the Security Official uses a method of erasing the media that irrecoverably destroys all data. The process of erasing the media is more secure than a simple format.

When a Communication Disorders Clinic information systems is removed from service, it undergoes at least eight swipes using the Army Corp of Engineers Data Removal Policy. The systems are rechecked at the warehouse for possible data.

**Implementation: Media Re-Use** (R) – implement procedures for removal of EPHI from electronic media before the media are made available for re-use. Videotapes, audiotapes, CD’s and DVD’s are considered a part of a client’s EPHI and are subject to the same safeguards to ensure the privacy and security. They are kept in the Clinic Office at the Clinic when not in use. Videotapes are not to be viewed outside of the Clinic. When viewed in the Clinic, the faculty member and/or graduate student should follow the same procedures for privacy and confidentiality as for client charts. Videotapes, CD’s, DVD’s and audiotapes being viewed/listened to are not to be left unattended by the workforce member. When leaving a workstation the video or audiotape recorder is to be turned off after removal of the tape. All used audiotapes are destroyed before being disposed of in the trash container. All used videotapes are hand carried to Media Services and are erased by one of the administrative staff members. DVD’s, although not extensively used to date, are destroyed before being discarded.

**Implementation: Accountability** (A) – maintain a record of the movements of hardware and electronic and any person responsible for them. All movement of Communication Disorders Clinic information systems and electronic media containing EPHI into, out of, and within its facilities must be appropriately tracked and logged. All media containing electronic PHI is checked out of the Clinic Office. Items to be disposed of or reused are given to the University Security Official in order to properly destroy the PHI on the media. Movement of hardware, either within the Clinic or when removed from the Clinic, is recorded with the University Security Official.
Implementation: Data Back-up and Storage (A) – create a retrievable, exact copy of electronic PHI, when needed, before movement of equipment. All client data entered on the Clinic networking system is subject to data back up every evening by the server which is housed in the Reich College of Education. The computer technical assistants are responsible for maintaining the security of the server as well as for data backup and storage.

Technical Security
Technical security involves the processes put in place to protect information, control and monitor information access, and to guard against unauthorized access to data transmitted over a communication network. These processes include audit controls, automatic computer log-off, and authentication measures such as the use of passwords and unique user identifications.

Technical security services are often governed by the particular technologies and data systems in use. Covered entities are expected to balance the need for timely access to needed health information with the need to protect its confidentiality and integrity. The rule provides for five areas of technical security services:

1. Access Control – providing controls limiting access to health information to those with valid needs and authorization.
2. Audit Controls – setting up system mechanisms that record and monitor activity.
3. Authorization Control – obtaining and tracking the consents of clients for use and disclosure of their health information.
4. Data Authentication – ensuring that data is not altered, destroyed, or inappropriately processed.
5. Entity Authentication – employing mechanisms such as automatic log-off, passwords, Personal Identification Numbers, and biometrics, which identify authorized users and deny access to unauthorized users.

Organizations that transmit health information over open networks must keep it from being easily intercepted by third parties via external entry points. Communications and network controls include:

1. Integrity Controls – internal verification that data being stored or transmitted is valid.
2. Message Authentication – assurance that messages sent and received are the same messages.
3. Either Access Controls – such as dedicated, secure communications lines – or Encryption – transforming text into unintelligible ciphers through the use of a special algorithm process.
4. If using a network, protections must also include alarms, audit trails, entity authentication, and event reporting.

Standard: Access Control – implement technical policies and procedures for electronic information systems that maintain EPHI to allow access only to those persons or software programs that have been granted access rights. The Communication Disorders Clinic information systems must support a formal process for granting appropriate access to Clinic information.
systems containing EPHI. Access to Communication Disorders Clinic information systems containing EPHI must be limited to Communication Disorders Clinic workforce members.

**Implementation: Unique User Identification (R)** – assign a unique name and/or number for identifying and tracking user identity. To maintain the security, integrity and confidentiality of all EPHI stored on the computer network system at the Clinic, workforce members are assigned a unique user ID number. This policy applies to all Clinic computer systems and applications and to all workforce members including faculty, administrative staff and graduate students. **Guests of the Clinic, primarily those observing therapy sessions for practicum purposes, are not permitted access to any computers in the Clinic for any purpose.** This includes access to user level accounts, web accounts, and e-mail accounts.

**Implementation: Emergency Access Procedure (R)** – establish (and implement as needed) procedures for obtaining necessary EPHI during an emergency. The Communication Disorders Clinic must have a formal, documented emergency access procedure enabling workforce members to access the minimum EPHI necessary to effectively and efficiently treat clients in the event of a major emergency. These may be different from those used under normal operational circumstances. The Clinic’s ability to access PHI following an emergency has been described in the Disaster Recovery Plan.

**Implementation: Automatic Logoff (A)** – implement electronic procedures that terminate an electronic session after a predetermined time of inactivity. To ensure the security of all electronic PHI at the Clinic, automatic locking procedures are programmed on all computers (including those of the faculty and staff, as well as those computers in the Student Work Room). When unattended, the computers at the Clinic automatically lock after 15 minutes of inactivity.

The Clinic cannot require that users are automatically logged off after a predetermined amount of time as a means of terminating an electronic session. Automatically logging users off workstations forces open documents to close without saving changes to that document. This potentially causes data corruption. Locking an idle computer after 15 minutes allows the original authorized user or the University Security Official to unlock it. Locking the workstation prevents any of the users’ EPHI from being accessed by non-authorized users but does not result in any loss or corruption of data as automatic logoffs potentially could cause.

**Implementation: Encryption and Decryption (A)** - implement a mechanism to encrypt and decrypt EPHI. Data encryption and decryption is not required. This is due primarily to the means by which catastrophic backups are obtained. This procedure does not allow for an encryption and/or decryption policy to be implemented.

**Standard: Audit Controls (R)** – implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use EPHI. Entities have flexibility to implement the standard in a manner appropriate to their needs as deemed necessary by their own risk analyses. All activity on machines storing EPHI is logged and all log files are retained permanently for any possible future use. The procedure for examination of log files is reviewed annually or as needed. Failed login attempts are filtered by the computer support staff in the Information Technology Services and forwarded to the University Security Official for review and documentation.

The server storing EPHI is located in a secured room locked at all times via a controlled lock and key. The University Security Official, other members of the Reich College of Education Information Technology group, and the Dean of the Reich College of Education are the only ones to maintain keys to this location.
Standard: Integrity – implement policies and procedures to protect EPHI from improper alteration or destruction. The Communication Disorders Clinic must appropriately protect the integrity of all EPHI contained on its information systems.

Implementation: Mechanism to Authenticate Electronic PHI (A) – implement electronic mechanisms to corroborate that EPHI has not been altered or destroyed in an unauthorized manner. The covered entities risk analysis must address what data should be authenticated, and to what degree of assurance. Access to EPHI, once approved by the appropriate workforce member (clinical faculty and staff), is limited. The Clinic does not utilize electronic client charts. All EPHI is converted to paper form and filed in the client’s chart.

Standard: Person or Entity Authentication (R) – implement procedures to verify that a person or entity seeking access to EPHI is the one claimed. Procedures for person or entity authentication are described above in Unique User Identification.

Standard: Transmission Security – implement technical security measures to guard against unauthorized access to EPHI that is being transmitted over an electronic communications network. Information concerning EPHI generated on the computer networking system at the Clinic is on file at the Clinic.

Implementation: Integrity Controls (A) – implement security measures to ensure that electronically transmitted EPHI is not improperly modified without detection until disposed of. A patient disclaimer allowing workforce members to contact someone by e-mail is in place before an e-mail is initiated. Procedures regarding other integrity controls are addressed elsewhere in this manual.

Implementation: Encryption (A) – implement a mechanism to encrypt EPHI whenever deemed appropriate. Data encryption and decryption is currently not implemented due to the means by which catastrophic backups are obtained.