Augsburg College HIPAA Policy

Policy Statement

The Administrative Safeguards portion of the Security Rule (collectively referred to as "Administrative Safeguards") addresses administrative measures and the policy and procedures for their use that protect ePHI and control access to it. It includes administrative actions, and policies and procedures, to manage the selection measures to protect electronic protected health information and to manage the conduct of the covered entity's workforce in relation to the protection of that information.

Policy Interpretation and Implementation

(A) Risk Analysis

Electronic protected health information is officially stored in only two places, the human resources network storage space and our Human Resources/Payroll system, Agresso. Despite in-place policies, it has the potential to exist in email, individually assigned network storage, and desktop/laptop computers. As a institution of higher learning, our network is relatively "open", inviting external probes and attacks. In addition, our residential student population serves a vector for network intrusion through spyware, viruses, and hacking. College employees also have wide latitude to use their computers in ways that may invite attacks through those same methods.

(B) Risk Management

Various security measures have been implemented to reduce risk and vulnerability to all of our information systems. These measures include:

(i) Policy on Computing Resources. This policy provides many guidelines for secure computing, including password requirements for confidentiality, prohibition against sharing account information, prohibition of attempts to access unauthorized information, and guidance on where to store sensitive information.

(ii) Policy on ePHI. The official policy of Human Resources prohibits the transmission of PHI over email and instant messaging. They will communicate PHI only over the telephone, written correspondence, or in-person.

(iii) Network Security. All servers are located behind an organization-wide firewall, allowing us to restrict access internally and externally to only authorized networks and individual computers.

(iv) Desktop Security. All college owned machines are required to have anti-virus and anti-virus software installing and operating at all times. We have implemented a patch management process to ensure all college owned machines are always up-to-date with security patches for applications and their operating system. Any machines that connect to our public and Residential Hall ports are also required to have anti-virus software. In addition, they are required to have the latest security updates for their operating system installed.

(C) Sanction Policy. All Violations of security policies and procedures are covered by existing rules in the Employee Handbook and/or Faculty Handbook.

(D) Information System Activity. All systems are required to implement logon auditing, permitting the Information Technology department to track both successful and unsuccessful logon attempts by time and date. Our Human Resources/Payroll system also audits information access and any changes to information within the system; including the time and date of the change, the change, and the user making the change. These logs are reviewed periodically.

(2) The role of HIPAA Security Officer is currently assigned to the Director for Information Technology Systems.

(3)(i) Workforce Security. Authorization to access electronic protected health information is only made upon request of the Human Resources department. The only Information Technology users with access are system administrators and the Human Resources assigned technician.

(ii) (a) Authorization. All users are assigned a single network account for access to the college network and any authorized network applications. Authorization is granted only on an as-needed basis, as determined either by their supervisor or the Information Technology department.

(b) Workforce Clearance. Work with electronic protected health information is performed exclusively

within the Human Resources department. Human Resources departmental policy regarding privacy of protected health information subsumes electronic protected health information handling.
(c) Termination Procedures. Upon termination, an employee's access to all information systems is suspended. The Human Resources department notifies a representative of the Information Technology of all impending terminations.
(4)(i) Information Access Management. See **(3)(i).**
(ii) (a) Not applicable.
(b) Access Authorization. Only Human Resources personnel are permitted to access electronic protected health information. Upon their guidance and request, new Human Resources employees are granted access to systems that may contain ePHI.
(c) Establishment and Modification. These features are provided by both our enterprise directories and Human Resources/Payroll system.
(5) Security Awareness and Training. The Human Resources department provided privacy training to a broad audience of employees and managers of the college regarding protected health information.
(a) Security Reminders.
(b) Protection from Malicious software. See **(B)(v)**.
(c) Log-in Monitoring. See **(D).**
(d) Password Management. See **(B)(i).**
(6)(i) Security Incident Procedures. Security incidents identified by unusual network activity, suspicious files or folders, or external reports are investigated by the network administrator and Director for Information Technology Systems.
(ii) Response and Reporting. All suspected or known compromises of information systems are addressed to the maximum effect to resolve the current compromise and address the vulnerability that permitted the original compromise. Reports of security compromises are maintained by the Director of Information Technology Systems.
(7)(i) Contingency Plan. The college maintains a disaster recovery plan that includes Information Technology specific recovery policies and plans.
(ii)(a) Data Backup Plan. Data backup of electronic protected health information is covered by the Information Technology department's published backup policy.
(b) Disaster Recovery Plan. See **(7)(i).**
(c) Emergency Mode Operation. See **(7)(i).**
(d) Testing and Revision Procedures. This process is included as part of the college-wide disaster recovery plan.
(e) Applications and Data Criticality. Critical electronic protected health information includes the Human Resources network stored files and Agresso data.
(8) Evaluation. Reviews of HIPAA security policies and procedures will be made in response to changes in our security environment or on an annual basis, whichever comes first.
(b) Business Associate Contracts. This standard is already met by Human Resources contracts.

References:
45 C.F.R. § 164.308

Physical Safeguards

Policy Statement

The Physical Safeguards portion of the Security Rule (collectively referred to as "Physical Safeguards") provide additional protection of ePHI. Physical safeguards are defined as "physical measures, policies, and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion."

Policy Interpretation and Implementation

(A)(1) Facility Access Controls. Server systems containing electronic protected health information are located exclusively in the Lindell Library server room. The only personnel with access to that facility are certain individuals of the Information Technology, Public Safety and Facilities departments. Access to the server room is only made on an as-needed basis.
(2)(i) Contingency Operations. See **Administrative Safeguards (7)**
(ii) Facility Security Plan. Policies regarding unauthorized physical access to secure locations are maintained by the Public Safety Department.
(iii) Access Control and Validation Procedures. All visitors to the server room must be accompanied by a representative of the Information Technology or Facilities departments. Normally, visitors are not permitted.
(iv) Maintenance Records. Records of maintenance work orders are kept by the Facilities Department.
(B) Workstation Use. The proper use of workstations is covered by the college's Use of Computing Resources Policy. In addition, the Human Resources department has specific departmental procedures to follow as they process electronic protected health information.
(C) Workstation Security. Physical safeguards, such as screen guards, are in use on workstations that process protected health information.
(D) Device and Media Controls. Prior to discarding or return, all workstations are re-imaged to remove all user data.
(2)(i) Disposal. It is the policy of the Information Technology department that user data is destroyed prior to disposal of equipment or media.
(ii) Media re-use. Relocated workstations are re-imaged as part of the relocation process. Backup media is re-used, but only as backup media and does not leave a protected environment.
(iii) Accountability. Assets are tracked through our asset management software system.
(iv) Data Backup and Storage. Backups are automatically generated every night and archived for 3 months or longer.

References:
45 C.F.R. § 164.310

Technical Safeguards

Policy Statement

The Technical Safeguards portion of the Security Rule (collectively referred to as "Technical Safeguards") addresses technology and requires policy and procedures for its use that protect ePHI and control access to it.

Policy Interpretation and Implementation

(A)(1) Access Control. Access control is provided by the use of our network directories and user group control within our Human Resources/Payroll software.
(2)(i) Unique User Identification. All faculty and staff are assigned unique usernames.
(ii) Emergency Access Procedure. Should emergency access be required, the emergency contact list should be used to contact a Director of Information Technology.
(iii) Automatic Logoff. Workstations that may process electronic protected health information will lock the desktop after 15 minutes of inactivity.
(iv) Encryption and Decryption.
(B) Audit Controls. See **Administrative Safeguards (D).**
(C)(1) Integrity. See **Administrative Safeguards (D).**
(2) Authentication of Information. See **Administrative Safeguards (D).**
(D) Person or Entity Authentication. To use any electronic resource, users are required to authenticate with their unique username and password. The use of someone else's username is explicitly prohibited.
(E) Transmission Security. Electronic protected health information is not routinely transmitted outside of communication with the college's health plan provider. Secure transmission of that information is provided by the provider.

References:
45 C.F.R. § 164.312