HIPAA Core Security Policy

Unit: Office of Information Technology  
Effective Date: 4/20/2005  
Revision Date: 10/22/2020  
Contact: J. Ashley Ewing  
Title: Chief Information Security Officer

Purpose

The purpose of this policy is to make sure that covered entities within The University of Alabama meet the requirements of HIPAA 45 CFR Part 160 and Subparts A and C of Part 164.

Policy

A covered entity must comply with all applicable HIPAA security standards, including but not limited to the following:

- Implement reasonable and appropriate procedures to comply with the standards, implementation specifications, or other requirements of the HIPAA Security Rule in writing either in paper records, or electronically. The documentation must be retained for at least six years from the date of the creation of the documentation, or the last date that the document was in effect, whichever is later.
- Comply with the security procedures to assist in providing appropriate administrative, technical and physical safeguards with respect to all ePHI.
  - Ensure the confidentiality, security, integrity, and availability of ePHI that it creates, receives, maintains, or transmits.
  - Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI and must protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required.
- Develop and implement reasonable and appropriate training related to the HIPAA Privacy and Security Rules.
- Disseminate all official updates of procedures to its workforce as applicable in a reasonably prompt time period.
- Periodically perform a risk assessment and develop a risk management plan.
- Review periodically, and update as needed, its policy, procedures, and other documentation in response to environmental or operational changes affecting the security of the ePHI.
- Follow the University of Alabama Incident Response Plan as it relates to HIPAA covered entities.

Violations of Policy

Violations of these policies may result in disciplinary action, up to and including dismissal, and civil and criminal penalties.

Vendors or contractors who do not follow the above policies may be subject to breach of contract penalties.

Business Associates must comply with UA policies applicable to the nature of their work with UA. Business Associates who do not follow applicable requirements could be subject to breach of contract penalties, possible legal prosecution, civil and criminal penalties, and other legal remedies/ramifications as are available to UA.

Definitions:

Business Associate (BA): A person or entity (other than an employee of a UA Covered Entity) who performs a function or activity involving the use or disclosure of protected health information, including, but not limited to, claims processing or administration, data analysis, processing or administration, utilization review, quality assurance,
billing, benefit management, practice management, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services, for or on behalf of a UA Covered Entity. A Business Associate of one UA Covered Entity does not become a Business Associate of any other UA Covered Entity simply by virtue of the UA Affiliation.

**HIPAA**: Health Insurance Portability and Accountability Act.

**HIPAA covered entity**: Any entity that furnishes, bills or receives payment for health care in the normal course of business, maintains ePHI and transmits covered transactions (such as insurance billing) electronically.

**Electronic Protected Health Information (ePHI or electronic PHI)**: Health information, including demographic information, collected from an individual and created or received by a health provider, health plan, employer, or health care clearinghouse that relates to the past, present, or future physical or mental health or condition of any individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual, that identifies an individual or there is a reasonable basis to believe the information can be used to identify the individual, and that is created, maintained, received or transmitted in any electronic format or media.

The following identifiers of an individual, or of relatives, employers, or household members of the individual, are considered ePHI:

1. Name
2. Geographic subdivisions smaller than a state; (street address, city, county, precinct, zip code, and equivalent geocode)
3. All elements of dates (except year) including birth date, admission and discharge dates, date of death, and all ages over 89 and all elements of dates (including year) indicative of such age
4. Telephone numbers
5. Fax numbers
6. Electronic mail address
7. Social security number
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/License numbers
12. Vehicle identifiers and serial numbers including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locator (URLs)
15. Internet protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code, except as allowed under the re-identification specifications (164.514(c)).

**Scope**

This entire Policy applies to UA Designated Health Care Components, UA departments serving as Business Associates for non-UA covered entities, covered health plans of The University of Alabama (a Covered Hybrid Entity) and to the administrative departments at The University of Alabama that provide legal, billing, auditing, or other administrative support for the above, including but not limited to The University of Alabama Office of Counsel, The University of Alabama System auditors, the University’s HIPAA Privacy and Security Officers, Office of Information Technology, Human Resources, and Risk Management.

For purposes of this Policy, these UA entities and their affiliated administrative support departments shall be referred to as “covered entity or entities” Compliance with this policy is required by all employees, volunteers, physicians, residents,
interns, trainees, contracted individuals, and other persons who work for a covered entity or are under the direct control of a covered entity, whether or not they are paid by the covered entity.

References

- 45 CFR Parts 160 and 164 HIPAA Administrative Simplification: Enforcement; Final Rule
- The University of Alabama HIPAA Procedures
- The University of Alabama Incident Response Plan

Office of the Provost

Signed: ___________________________ 10/22/2020
Joel Brouwer
Associate Provost