

ADMINISTRATIVE DIVISION UNIV University Administration		POLICY NUMBER UNIV 1.60
POLICY TITLE HIPAA Compliance		
SCOPE University System	DATE OF REVISION July 05, 2019	
RESPONSIBLE OFFICER General Counsel	ADMINISTRATIVE OFFICE Office of General Counsel	

PURPOSE

This policy is being promulgated to assure compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the HIPAA Omnibus Rule (January 2013), the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, and other applicable regulations.

This policy supplements the requirements of the Family Educational Rights and Privacy Act (FERPA) and any applicable South Carolina privacy and security laws.

This policy updates the existing university HIPAA Health Care Components and defines required procedures for those Health Care Components. This policy also defines required procedures for University Business Associates who have signed agreements to access PHI belonging to an outside HIPAA Covered Entity.

DEFINITIONS AND ACRONYMS

For all HIPAA terminology used in this policy, the university incorporates the definitions set forth in the HIPAA regulations at 45 CFR Parts 160, 162, and 164.

Business Associate is a person or entity, other than a member of the workforce of a covered entity or component, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to PHI. (45 CFR § 160.103).

Business Associate Agreement (BAA) is a contract between a covered entity and a business associate whereby the business associate agrees to protect the covered entity’s PHI in accordance with HIPAA and HITECH guidelines, if applicable. (45 CFR 164.504(e)).

Covered entity or covered component means (1) a health plan, (2) a health care clearinghouse, or (3) a health care provider who transmits any health information in electronic form in connection with a covered transaction. (45 CFR § 160.103).

Health Care Component means a component or combination of components of a hybrid entity designated by the hybrid entity. Health care components must include any component that would

meet the definition of a covered entity or business associate if it were a separate legal entity. (45 CFR § 164.103; 45 CFR § 164.105).

Hybrid Entity: means a single legal entity; (1) that is a covered entity; (2) whose business activities include both covered and non-covered functions; and (3) that designates health care components. (45 CFR § 164.103).

Individually Identifiable Health Information is information that is a subset of health information, including demographic information collected from an individual, and (1) is created or received by a health care provider, health plan, employer, or health care clearinghouse, and (2) relates to the past, present, or future physical or mental condition of an 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; and (i) that identifies the individual; or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual. (45 CFR § 160.103).

Notice of Privacy Practices (NPP) assures an individual has a right to adequate notice of the uses and disclosures of PHI that may be made by the hybrid entity, and of the individual's rights and the hybrid entity's duties with respect to PHI. (45 CFR § 164.520).

Protected Health Information (PHI) means individually identifiable health information that is: (1) transmitted by electronic media, (2) maintained in electronic media, (3) transmitted or maintained in any other form or medium. PHI does not include individually identifiable health information in education records covered by FERPA. (45 CFR § 160.103).

POLICY STATEMENT

- A. The university has elected to be a Hybrid Entity under HIPAA and hereby designates those facilities listed in **Appendix 1** as Health Care Components or HIPAA Covered Entities. These Health Care Components must comply with the standards and required implementation specifications of the HIPAA Privacy and Security Rules.

- B. This policy also applies to those university departments, clinics, research centers, or individuals that have signed Business Associate Agreements (BAAs) with outside covered entities. The university units functioning as Business Associates are subject to the HIPAA Security Rule and parts of the Privacy Rule as reflected within the corresponding BAA. These Business Associates must comply with the standards and required implementation specifications of the HIPAA Security Rule. However, being a party to a BAA with an outside covered entity does not make that department or unit a health care component for purposes of university's hybrid designations.

- C. All other university departments or components may voluntarily choose to comply with or participate in some or all aspects of this HIPAA policy, but such compliance or participation will not affect the department's status as a non-covered unit. The College of Nursing and the School of Medicine in Columbia and the School of Medicine in Greenville all employ clinical faculty who are separately engaged in the practice of medicine pursuant to arrangements with independent medical practice organizations. As the medical practice functions as a separate legal entity from the university, neither the College of Nursing nor the Schools of Medicine in Columbia and Greenville are included within the university's Health Care Component designations.

PROCEDURES

- A. The Privacy Officials designated by the Health Care Components are responsible for adopting and implementing their respective policies and procedures for HIPAA compliance and for posting a Notice of Privacy Practices (NPP) on the respective health care component's website. The Privacy Officials are designated to receive complaints under this policy and to provide further information about matters covered by the health care component's NPP.
- B. The Director of HIPAA Compliance and the university HIPAA Committee will assist the Privacy Officials with developing policies and procedures for HIPAA compliance. The HIPAA Committee is constituted with the Privacy Officials of the Health Care Components, the Director of HIPAA Compliance, a representative from the Division of Information Technology Security, and a representative from each university unit, department, or center that is party to a BAA with an outside covered entity. Other members may be added at the discretion of the Director of HIPAA Compliance.
- C. All Health Care Components are responsible for developing operating procedures and forms as needed to implement and comply with applicable HIPAA regulations, including appropriate administrative, technical and physical safeguards to protect the privacy of protected health information. All Health Care Components must provide the Director of HIPAA Compliance with copies of their current policies and procedures and any forms or other HIPAA-related documents. The Director of HIPAA Compliance may require a Health Care Component to change its procedures, forms, or related documents.
- D. Health Care Components must also submit an Annual HIPAA Report to the Office of the President and the Director of HIPAA Compliance. This annual HIPAA Report will document the compliance efforts of each Health Care Component. The report must be formatted to conform to the [Annual HIPAA Report template](#).
- E. Business Associate Agreements (BAAs) with outside entities or vendors must be in writing and must contain university-approved HIPAA compliant language and authorized signatures.

Accordingly, any university faculty or staff who desires to execute a BAA with an outside entity or vendor must send the proposed BAA to the Director of HIPAA Compliance in the Office of General Counsel for review and approval. It is the responsibility of the Privacy Officers of each Health Care Component to assure that valid BAAs are executed when contracting with third parties with whom PHI will be shared.

- F. All university departments, clinics, centers, units, or employees functioning as HIPAA Business Associates must designate a HIPAA Security Officer for purposes of compliance with the HIPAA Security Rule. The HIPAA Security Officer designated by each university Business Associate must draft a policy and procedure manual addressing the HIPAA Security Rule implementation specifications applicable to the project. The Business Associate policy and procedure manual must be sent to the Director of HIPAA Compliance for review and comment prior to accessing PHI or ePHI pursuant to the BAA. The Director of HIPAA Compliance may require a Business Associate to change its procedures, forms, or related documents.

- G. The Division of Information Technology (DoIT) is responsible for regularly monitoring and testing the university network. DoIT representatives will assist Health Care Components and Business Associates to coordinate the university's compliance with HIPAA's security rule and to consult regarding the implementation of required security controls of systems authorized to process, transmit, and store PHI.

- H. HIPAA establishes privacy protections and establishes the conditions under which protected health information (PHI) may be used or disclosed by Covered Entities, including university's Covered Components, for research purposes. It is the responsibility of the Covered Entity's Privacy Officer to ensure compliance with all regulatory requirements prior to using or disclosing PHI for research purposes. Such compliance will require that a university researcher adhere to terms and conditions imposed by the Covered Entity. Researchers with questions about HIPAA compliance may contact the Director of HIPAA Compliance for additional guidance.

- I. Complaints concerning HIPAA policies and procedures and/or compliance with those policies and procedures will be made in writing to the Director of HIPAA Compliance. The Director of HIPAA Compliance will investigate all complaints in a timely manner and provide a written determination to the parties involved (e.g., the complainant and the subject covered units) and to the Privacy Official. The Privacy Official (for Health Care Components) or Security Officer (for Business Associates) will implement corrective actions, as appropriate, and amend policies and procedures accordingly.

- J. All Health Care Components and Business Associates will train workforce members (faculty, staff, students and volunteers) on policies and procedures with respect to PHI as required by HIPAA. Such training will be as necessary and appropriate for the members of the staff to carry out their functions and must be provided within a reasonable time after joining the workforce. The Privacy Officials of each covered Health Care Component are responsible for overseeing the adoption of training materials, implementation of staff training, and maintenance of training records. For Business Associates, the designated Security Officer is responsible for overseeing the adoption of training materials and the implementation of staff training.

- K. Individuals will not be required to waive any of their rights, or the right to file a complaint under the HIPAA privacy regulations as a condition of treatment, payment, enrollment in a health plan, or eligibility for benefits.

- L. The university will mitigate, to the extent practicable, any known harmful effect of the use or disclosure, by the university or its business associates, of PHI in violation of its policies and procedures or the HIPAA privacy regulations.

- M. Violation of this policy by a member of the university’s workforce is subject to appropriate personnel or other disciplinary action.

- N. All policies, procedures, communications, actions, activities and/or designations that require documentation under HIPAA must be maintained in written and/or electronic form and retained for a period not less than six years from the date of its creation or the date when it was last in effect, whichever is later.

RELATED UNIVERSITY, STATE AND FEDERAL POLICIES

[BTRU 1.04 Authority to Sign Contracts](#)

[RSCH 1.03 Research and Human Subjects](#)

[HITECH – Public Law 111-005 42 U.S.C. § 17921, et seq.](#)

[HIPAA – Public Law 104-191 45 C.F.R. Parts 160, 162, and 164](#)

HISTORY OF REVISIONS

DATE OF REVISION	REASON FOR REVISION
July 05, 2019	New policy

APPENDIX

The University of South Carolina’s Hybrid Health Care Components or HIPAA Covered Entities

APPENDIX 1

The University of South Carolina's Hybrid Health Care Components or HIPAA Covered Entities are:

1. Student Health Services ("SHS"), including the Center for Health and Wellbeing and Counseling and Psychiatry, located in Columbia, SC.
2. Speech & Hearing Research Center ("SHRC"), doing business as "Montgomery Speech Language and Hearing Clinic" as of June 1, 2019, located in Columbia, SC.
3. Upstate Health Services ("Upstate Health Services") located in Spartanburg, SC.
4. Upstate Counseling Services ("Upstate Counseling Services") located in Spartanburg, SC.

Effective July 05, 2019