1. **Purpose**

1.1. The purpose of this rule is to provide guidance on when an East Carolina University Health Care Component (“ECU Health Care Component”) is required to enter into a Business Associate Agreement (“BAA”) in accordance with the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). ECU Health Care Components that create or maintain Protected Health Information (“PHI”) are required to enter into a BAA (i) with an entity performing functions or services on behalf of such Health Care Component; or (ii) with an entity which is acting as a vendor of personal health records. There may be situations in which a BAA is required between ECU’s Health Care Components and other non-health care components of ECU.

2. **Definitions**

2.1. **Business Associate** means:

2.1.1. With respect to an ECU Health Care Component, a Person who:

2.1.1.1. On behalf of an ECU Health Care Component or an Organized Health Care Arrangement in which an ECU Health Care Component participates, but
other than in the capacity of a Workforce member, creates, receives, maintains, or transmits PHI for a function or activity including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, and re-pricing; or

2.1.1.2. Provides, other than in the capacity of a workforce member of an ECU Health Care Component, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such covered entity, or to or for an Organized Health Care Arrangement in which an ECU Health Care Arrangement participates, where the provision of the service involves the disclosure of PHI from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.

2.1.2. An ECU Health Care Component may be a Business Associate of another covered entity.

2.1.3. Business Associate includes:

2.1.3.1. A health information organization, e-prescribing gateway, or other person that provides data transmission services with respect to PHI to an ECU Health Care Component and requires access on a routine basis to such PHI.

2.1.3.2. A person that offers a personal health record to one or more individuals on behalf of an ECU Health Care Component.
2.1.3.3. A subcontractor that creates, receives, maintains, or transmits PHI on behalf of another Business Associate.

2.1.4. Business Associate does not include:

2.1.4.1. A health care provider, with respect to disclosures by an ECU Health Care Component to the health care provider concerning the treatment of the individual.

2.1.4.2. A Plan Sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of 45 CFR 164.504(f) are met.

2.1.4.3. A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting PHI for such purposes, to the extent such activities are authorized by law.

2.1.4.4. An ECU Healthcare Component participating in an Organized Health Care Arrangement that performs a function or activity, as described in paragraph 2.1.1.1, for or on behalf of such Organized Health Care Arrangement, or that provides a service, as described in paragraph 2.1.1.2, to or for such Organized Health Care Arrangement by virtue of such activities or services.

2.2. Business Associate Agreement means a formal and written agreement in which the Business Associate provides assurance that it will appropriately safeguard the PHI of an ECU Health Care Component. The agreement serves to clarify and limit, as appropriate, the permissible uses and disclosures of PHI by the Business Associate based on its
relationship with an ECU Health Care Component and the activities or services being performed by the Business Associate.

2.3. **Data aggregation** means, with respect to protected health information created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such protected health information by the business associate with the protected health information received by the business associate in its capacity as a business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

2.4. **Health Insurance Portability and Accountability Act of 1996 ("HIPAA")** means provisions developed by the Department of Health and Human Services to provide a uniform federal floor for privacy protections.

2.4.1. **HIPAA Privacy Rule** means a national standard to protect individuals’ medical records and other personal health information and applies to health plans, health clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Privacy Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Privacy Rule also gives patients certain rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

2.4.2. **HIPAA Security Rule** means a national standard to protect individuals’ electronic personal health information that is created, received, used, or maintained by a covered entity. The Security Rule requires appropriate administrative, physical
and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information.

2.5. **Organized Health Care Arrangement** means:

2.5.1. A clinically integrated care setting in which individuals typically receive health care from more than one health care provider; or

2.5.2. An organized system of health care in which more than one covered entity participates and in which the participating covered entities (i) hold themselves out to the public as participating in a joint arrangement; and (ii) participate in joint activities that include at least one of the following:

2.5.2.1. Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;

2.5.2.2. Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or

2.5.2.3. Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if PHI created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

2.6. **Patient Safety Activities** means the following activities carried out by or on behalf of a patient safety organization or a provider:
2.6.1. Efforts to improve patient safety and the quality of health care delivery;

2.6.2. The collection and analysis of patient safety work product;

2.6.3. The development and dissemination of information with respect to improving patient safety, such as recommendations, protocols, or information regarding best practices;

2.6.4. The utilization of patient safety work product for the purposes of encouraging a culture of safety and of providing feedback and assistance to effectively minimize patient risk;

2.6.5. The maintenance of procedures to preserve confidentiality with respect to patient safety work product;

2.6.6. The provision of appropriate security measures with respect to patient safety work product;

2.6.7. The utilization of qualified staff; and

2.6.8. Activities related to the operation of a patient safety evaluation system and to the provision of feedback to participants in a patient safety evaluation system.

2.7. **Person** means a natural person, trust or estate, partnership, corporation, professional association or corporation or other legal entity, public or private.

2.8. **Plan Sponsor** means:

2.8.1. The employer in the case of an employee benefit plan established or maintained by a single employer;
2.8.2. The employee organization in the case of a plan established or maintained by an employee organization; or

2.8.3. In the case of a plan established or maintained by two or more employers or jointly by one or more employers and one or more employee organizations, the association, committee, joint board of trustees, or other similar group of representatives of the parties who establish or maintain the plan.

2.9. **Protected Health Information** means:

2.9.1. Individually identifiable information, that is a subset of health information, including demographic information collected from an individual, and:

2.9.1.1. is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

2.9.1.2. relates to the past, present, or future physical or mental health or condition of a subject; the provision of health care to a subject; or the past, present, or future payment for the provision of health care to a subject; and

2.9.1.2.1. That identifies the subject; or

2.9.1.2.2. With respect to which there is reasonable basis to believe the information can be used to identify the individual.

2.9.2. PHI can be:

2.9.2.1. Transmitted by electronic media;

2.9.2.2. Maintained in electronic media; or

2.9.2.3. Transmitted or maintained in any other form or medium.
2.9.3. PHI excludes individually identifiable information that is

2.9.3.1. In education records covered by the Family Educational Rights and Privacy Act, as amended, 20. U.S.C. 1232g;

2.9.3.2. In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);

2.9.3.3. In employment records held by a covered entity in its role as employer;

and

2.9.3.4. Regarding a person who has been deceased for more than 50 years.

2.10. **Workforce** means employees, volunteers, trainees, learners, faculty, students and other persons whose conduct in the performance of work for an ECU Health Care Component, is under the direct control of such ECU Health Care Component, whether or not they are paid by the ECU Health Care Component.

3. **Policy**

3.1. From time to time, ECU Health Care Components may share PHI with external parties, referred to as Business Associates. It is the policy of ECU’s Health Care Components that PHI may only be shared with Business Associates pursuant to an approved BAA.

4. **Procedure**

4.1. It is the responsibility of each department, division, or operating unit contracting for services with third parties with which identifiable PHI will be shared, to assure that valid Business Associate Agreements are executed.

4.1.1. For more information regarding the determination of whether a Business Associate Agreement is needed, please refer to the privacy forms section of the ECU HIPAA Privacy
website for a detailed step-by-step process for determining if a Business Associate Agreement is required.

4.2. Business Associate Agreements must be in writing using ECU’s approved Business Associate Agreement. These can be initiated at the unit level as part of the normal contracting/agreement process.

4.3. Any deviation from the standard Business Associate Agreement template must be reviewed by the ECU HIPAA Privacy Officer who may consult with the Office of University Counsel prior to signing the agreement.

4.4. All ECU Business Associate Agreements must only be signed by the Vice Chancellor for Health Sciences or delegees which can include: the Senior Associate Vice Chancellor for Medical Affairs and the Dean of BSOM, the Executive Associate Vice Chancellor for Health Sciences Administration and Finance, or the Associate Vice Chancellor for Healthcare Regulatory Affairs.

4.5. Business Associate Agreements shall be maintained with the underlying contract by the department, division, or operating unit contracting for services.

4.6. The department, division, or operating unit contracting for services must provide the executed Business Associate Agreement to the ECU HIPAA Privacy Office.

4.7. At any time if ECU suspects that a Business Associate has breached a material term or obligation under the agreement relating to HIPAA compliance, the department that is party to the agreement and the ECU HIPAA Privacy Officer must be notified and shall seek to immediately remedy such breach or, if that is not possible, to alter or terminate the Business Associate Agreement. Violations may also be reported by ECU to the Department of Health and
Human Services, Office for Civil Rights, as part of reviews conducted by the Office of the University Counsel, Risk Management, Office of Institutional Integrity, and the ECU HIPAA Privacy Officer, as necessary.