UNIVERSITY OF SOUTHERN MAINE
Office of Research Integrity & Outreach

Procedure #:	HIPAA-001; HRPP-016
AAHRPP:	Element II.3.D.
Date Adopted:	03/03/2017
Last Updated:	04/16/2020
Updated By:	
Prepared By:	Casey Webster
Reviewed By:	RSC, ORIO, System Counsel, HIPAA Security Official
Procedure Title:	**USM as Business Associate Component**

1.0 Objective

1.1. The objective of this Standard Operating Procedure (SOP) is to describe the policies and procedures for a University of Southern Maine (USM) Business Associate Component to receive, obtain, use, or disclose any Protected Health Information (PHI) from or on behalf of an external Covered Entity.

2.0 General Description

2.1. The University of Southern Maine is committed to ensuring compliance with the privacy and security safeguards set forth under the Health Insurance Portability and Accountability Act (HIPAA). ORIO Guidance and Resources

2.2. Units within USM (departments, schools, offices, or other units) may provide services to an external HIPAA Covered Entity. Such services may cause the USM unit to meet the definition of a Business Associate with respect to that external Covered Entity. As required by HIPAA, USM may only provide such business associate services to an external Covered Entity pursuant to a written Business Associate Agreement (BAA), which includes specific assurances.

2.3. A USM Business Associate Component shall not receive, obtain, use or disclose any PHI from or on behalf of an external Covered Entity unless and until a written BAA has been approved by UMS General Counsel and has been signed by both parties.

2.4. A BAA is appropriate only if the intended relationship with the external Covered Entity actually falls within the definition of Business Associate. In all other cases, a department, school, office or any other unit within the University of Southern Maine may create, receive, maintain, or transmit PHI from or on behalf of the Covered Entity only if:

2.4.1. The individual has given written authorization or

2.4.2. The HIPAA Privacy Rule permits the intended use and disclosure of PHI without the individual's authorization (e.g., for treatment, payment, or health care operations purposes); or

2.4.3. The use or disclosure is for research and a waiver of individual authorization has been approved by a HIPAA Privacy Board or Institutional Review Board.

3.0 Definitions

3.1. Business Associate means, with respect to a Covered Entity, a person who:

3.1.1. On behalf of such Covered Entity or an Organized Health Care Arrangement (OHCA), but other than in the capacity of a member of the workforce of such Covered Entity, creates, receives, maintains or transmits PHI for a function or activity regulated by HIPAA, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, and repricing;

3.1.2. Provides, other than in the capacity of a member of the workforce of such Covered Entity, legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation, or financial services to or for such Covered Entity or an OHCA, where the provision of the service involves the disclosure of PHI from such Covered Entity or OHCA, or from another Business Associate of such Covered Entity or OHCA, to the person; or

3.1.3. A subcontractor that creates, receives, maintains or transmits PHI on behalf of a business associate.

3.2. Business Associate Component means a department, school, office or any other unit within the University of Maine System that meets the definition of a Business Associate with respect to an external Business Associate or Covered Entity.

3.3. Covered Entity means one of the following:

3.3.1. A health plan

3.3.2. A health care clearinghouse

3.3.3. A health care provider who transmits any health information in electronic form in connection with a covered transaction.

3.4. Individually Identifiable Health Information means information that is a subset of health information, including demographic information collected from an individual, and:

3.4.1. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

3.4.2. Relates to the past, present, or future physical or mental health or 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

3.4.2.1. That identifies the individual; or
3.4.2.2. With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

3.5. Protected Health Information (PHI) means individually identifiable health information:

3.5.1. Except as provided in (2) of this definition, that is:

3.5.1.1. Transmitted by electronic media;
3.5.1.2. Maintained in any medium described in the definition of electronic media; or
3.5.1.3. Transmitted or maintained in any other form or medium

3.5.2. PHI excludes individually identifiable health information in:

3.5.2.1. Education records covered by FERPA (20 U.S.C. 1232g);
3.5.2.2. Records on a student who is eighteen years of age or older, or is attending an institution of postsecondary education, which are made or maintained by a physician, psychiatrist, psychologist, or other recognized professional or paraprofessional acting in their professional or paraprofessional capacity or assisting in that capacity, and which are made, maintained, or used only in connection with the provision of treatment to the student, and are not available to anyone other than persons providing such treatment, except that such records can be personally reviewed by a physician or other appropriate professional of the student's choice;
3.5.2.3. Employment records held by a Covered Entity in its role as employer; and
3.5.2.4. Regarding a person who has been deceased for more than fifty (50) years.

4.0 Responsibility

4.1. It is the responsibility of the Research Service Center (RSC) to execute this SOP.

4.2. The Business Associate Component shall comply with all of the terms and conditions of the BAAs into which it enters.

4.3. The Business Associate Component shall take all reasonable measures to ensure compliance with the terms and conditions of the BAA and shall take prompt and appropriate action in the event of any breach of the agreement.

4.4. The Business Associate Component shall not disclose any PHI to a business associate that is a subcontractor, or permit a business associate that is a subcontractor to create, receive, maintain, or transmit PHI on its behalf unless the Business Associate Component obtains satisfactory written assurances in the form of a business associate contract that the subcontractor will appropriately safeguard the information.

5.0 Procedure

5.1. Draft Required Documentation

5.1.1. The Business Associate Component will draft a memorandum (BAA Memorandum) that will include the following information:

5.1.1.1. The identity of all parties involved in the providing of services, which parties are Covered Entities, and the formal relationship between the parties;
5.1.1.2. The Individually Identifiable Information that will be used, disclosed or created, from whom the information will be acquired, obtained, or collected;
5.1.1.3. The purpose of the services to be provided, including goals, deliverables, and the scope of work;
5.1.1.4. Any associated contracts; and
5.1.1.5. A proposed BAA.
5.1.1.5.1. The proposed BAA will be drafted by the external Covered Entity.
5.1.1.5.2. It is the responsibility of the Business Associate Component to ensure the proposed BAA includes terms comparable to the UMS BAA template found within the ORIO Guidance and Resources.

5.2. Consult with the HIPAA Security Official

5.2.1. The Business Associate Component will send the BAA Memorandum to the HIPAA Security Official for feedback.

5.2.2. The HIPAA Security Official will review the proposed BAA and notify the Business Associate Component of any required changes.

5.2.3. The Business Associate Component will incorporate any required modifications into the proposed BAA.

5.3. Obtain Approval from the University of Maine System Counsel

5.3.1. The Business Associate Component will send the BAA Memorandum (after HIPAA Security Official review) to the University of Maine System Office of General Counsel (System Counsel) for approval.

5.3.2. System Counsel will review the proposed BAA and notify the Business Associate Component of any required changes.

5.3.3. The Business Associate Component will incorporate any required modifications and send an updated proposed BAA to the System Counsel for approval.

5.3.4. System Counsel will inform the Business Associate Component of approval of the proposed BAA.

5.3.4.1. System Counsel may determine that the proposed BAA is not required but request one of the following be obtained instead:

5.3.4.1.1. Data Use Agreement

5.3.4.1.2. Individual Authorization

5.3.4.1.3. A Waiver of Individual Authorization

5.4. Obtain Required Signatures

5.4.1. The Business Associate Component will send the proposed BAA that has been approved by System Counsel to the Research Service Center.

5.4.2. The Director of the Research Service Center (RSC) will complete a final review of the proposed BAA and sign the BAA or delegate the Assistant Provost for Research Integrity to sign on behalf of USM.

5.4.2.1. In the event that the Director requires changes to the proposed BAA, the Business Associate Component will send the modified BAA to System Counsel for approval before obtaining the Director's signature.

5.4.3. Once a signature has been obtained on behalf of USM, the Business Associate Component will send the BAA signed by USM to the Covered Entity for signature.

5.4.3.1. In the event that the Covered Entity requires changes to the BAA, the Business Associate Component will send the modified BAA to System Counsel for approval before obtaining the Director of RSC and Covered Entity signatures.

5.5. Forward Documentation to the ORIO

5.5.1. The Business Associate Component will send a final copy of the BAA Memorandum, including the BAA signed by both parties, to both the ORIO and RSC.

5.5.2. The Business Associate Component will send a final copy of the BAA Memorandum, including the BAA signed by both parties, to the Office of Research Integrity and Outreach.

5.5.3. The Business Associate Component will maintain a final copy of the BAA Memorandum, including the BAA signed by both parties, and attach the BAA Memorandum when requested for any RSC or ORIO submission.

5.6. Complete Required Training

5.6.1. The Business Associate Component will ensure all named personnel under the BAA Memorandum complete the Health Information Privacy and Security (HIPS) Course through the Collaborative Institutional Training Initiative.

5.7. Changes to an Existing BAA

5.7.1. In the event that the Business Associate Component or Covered Entity wishes to make any changes to the BAA, the Business Associate Component must again obtain HIPAA Security Official review, System Counsel approval, required signatures, and forward documentation to the RSC and ORIO.

6.0 References

6.1. University of Maine System HIPAA Policies and Forms