

## **BUSINESS ASSOCIATE AGREEMENT PROCEDURES**

### **I. DEFINITIONS**

**Business Associate** is a person or entity who is not a member of EMU's workforce, who creates, receives, maintains, or transmits Protected Health Information for a function or activity regulated by HIPAA on behalf of a covered entity (e.g. EMU hybrid covered entity).

Business Associate relationship examples: some technical vendors with access to computing infrastructures containing PHI, Cloud Service Providers, Data Transcription Service Providers, Accreditation Organizations, Health Information Exchanges (HIE), Patient Safety Organizations (PSO) and persons or entities providing legal, actuarial, accounting, consulting, data aggregation, management, administrative, or financial services claims processing or administration, data analysis, research, processing or administration, utilization review, quality assurance, patient safety activities listed at 42 CFR 3.20, billing, benefit management, practice management, and repricing.

A **Business Associate Agreement** documents assurances from the outside party (business associate) that it will not use or disclose the EMU's PHI except as permitted by the EMU or as permitted by law.

### **II. POLICY STANDARDS**

A. Prior to disclosing any Protected Health Information (PHI) to a Business Associate, EMU will obtain satisfactory assurances from a Business Associate that the Business Associate will appropriately safeguard the PHI it receives or creates on behalf of EMU. EMU will document these satisfactory assurances in writing in the form of a Business Associate Agreement (BAA) with the Business Associate in compliance with the HIPAA regulations.

**New Contracts.** The general Business Associate process is illustrated below:

- a. Contracts that may require business associate agreements shall be routed to the appropriate processing unit / authorized signer. Procurement shall send the unit/authorized signer EMU's BAA Questionnaire to assist the Legal Affairs Office in determining the necessity for a BAA. Procurement shall send the completed questionnaire to the Legal Affairs Office for a determination as to whether a BAA is necessary. If a BAA is necessary, Procurement may process the Business Associate Agreement as long as no material changes are made. Approval of the Legal Affairs Office is required if there is any material deviation from the EMU Business Associate Agreement, or the supplier's business associate agreement is used instead of the EMU Business Associate Agreement.
- b. **The EMU Business Associate Agreement** shall be presented to suppliers as the preferred option.
- c. **Authority to Execute Business Associate Agreements.** Only persons authorized under EMU's Signatory Policy may execute a Business Associate Agreement, and only in compliance with the provisions of this policy.
- d. Third party/vendors expressing concerns or indicating that negotiation is needed will be referred to the Office of Legal Affairs.

B. **Business Associate Agreement:** A Business Associate Agreement shall require Business Associates to implement administrative, physical and technical safeguards that reasonably and appropriately

protect the confidentiality, integrity, and availability of protected health information that they create, receive, maintain, or transmit on behalf of the covered entity as required by the HIPAA Privacy and Security Rule, and must ensure that any agent, including subcontractor, to whom they provide such information, agrees to implement reasonable and appropriate safeguards to protect it.

- **Designated Record Set:** To the extent the Business Associate maintains PHI in a *Designated Record Set*, the Business Associate will cooperate with EMU to honor patient rights as mandated by the Privacy Rule in accordance with the required timelines for response.
- **Disclosures to Business Associates.** EMU may disclose PHI to a business associate, though only as necessary to enable the business associate to carry out its function and not for the Business Associate's independent use or purposes.
- **Safeguarding PHI.** The business associate agreement shall require the business associate to safeguard the PHI in accordance with the requirements of the *HIPAA Privacy Standards* at 45 C.F.R. Â§ 164.504(e)(1). See [Business Associate Agreement](#) for standard business associate agreement provisions.
- **Uses and Disclosures by Business Associates.** A business associate may use and disclose PHI only:
  - as permitted for the purposes set forth in the business associate agreement;
  - for the proper management and administration of the business associate;
  - if expressly permitted by the terms of the business associate agreement, the business associate may provide data aggregation services relating to UMHS's health care operations;
  - to carry out the legal responsibilities of the business associate; and
  - as otherwise specified in the business associate agreement.

EMU shall inform a business associate of changes to its use and disclosures of PHI in its notice if it affects the business associate's use or disclosure.

**III. Violation of Business Associate Agreements.** EMU is not required to monitor its Business Associates for compliance with their business associate agreements. If EMU obtains knowledge that a Business Associate has engaged in activity that is a material violation of the Business Associate's obligations under the business associate agreement, EMU shall require its Business Associate to take reasonable steps to cure the breach or end the violation. If continuing violations occur, EMU shall terminate the contract if feasible, and shall report the violation to the Secretary of Health and Human Services.

**EMU as a Business Associate.** If any unit or school obtains outside PHI from another covered entity, under circumstances which, by the above definition, EMU has been confirmed to be a BA: EMU's Privacy Officer shall obtain and review a written explanation from that covered entity justifying their designation of EMU as their business associate.

**Covered Components Added to the Covered Entity.** If a unit of EMU is added to the covered entity, The Privacy Officer or his or her designee(s), with assistance from the Office of Legal Affairs, shall review that unit's contracts with outside suppliers that involve use or disclosure of PHI in order to determine whether such contracts/relationships need to include business associate agreement provisions.

### **III. EXHIBITS**

Business Associate Agreement Process -

#### **Business Associate Agreement Templates:**

A. Business Associate Agreement Template (EMU as Covered Entity) - Updated xx/xx/xx

B. Business Associate Agreement Template (EMU as Business Associate) - Updated xx/xx/xx

### **VII. REFERENCES**

None

#### **Author:**

#### **Approved**

Reference: 45 C.F.R. Â§Â§ 164.520(b)(1)(vii), 164.524(d)(2)(iii), 164.526(d)(1)(iv), 164.530(a)(1)(ii) (2001)

65 Fed. Reg. 82462, 82548, 82550, 82557, 82561-62, 82747 (Dec. 28, 2000); 67 Fed. Reg. 53182-273 (Aug. 14, 2002)

Resources:

<http://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html>