UMHS Policy 01-04-400
Business Associate Agreements


I. POLICY STATEMENT, PURPOSE AND SCOPE

HIPAA requires that covered entities (health care providers) enter into contracts with their business associates to ensure that the business associate will appropriately safeguard the privacy and security of UMHS patient protected health information.

It shall be the policy of the University of Michigan Health System (UMHS) to enter into a written business associate agreement with any person or entity, other than a member of UMHS' workforce, who performs functions or activities on behalf of UMHS that requires access to patient protected health information.

The purpose of this policy is to protect the patient, the clinical team, and UMHS from inappropriate use and disclosure of protected health information.

This policy applies to all workforce members of UMHS except MHC and those subsidiaries and joint ventures of MHC that are not affiliated covered entities of the University or included in the University's organized health care arrangement and refers to all information resources, whether verbal, printed, or electronic, and whether individually controlled, shared, stand-alone or networked. Proper handling of external requests for patient information is addressed in UMHS Policy 01-04-310, Release of Protected Health Information under an Authorization.

II. DEFINITIONS

See UMHS Policy 01-04-300, Introduction to Privacy and Security Concepts and Definitions, for the definitions of italicized terms. Terms are only italicized the first time they appear in a given policy.

**Business Associate** - A person or entity that creates, receives, maintains, or transmits Protected Health Information on behalf of a covered entity. A Business Associate is not a member of the covered entity’s workforce. UMHS is a covered entity because it provides health care services.

Business Associate relationship examples: technical vendors with access to UMHS computing infrastructures containing PHI, cloud service providers, data transcription service providers, accreditation organizations, health information exchanges (HIEs), Patient Safety Organizations (PSOs), and persons or entities providing legal, actuarial, accounting, consulting, data aggregation, management, administrative, or financial services on behalf of UMHS.
Business Associate Agreement - Documents assurances from the outside party (Business Associate) that it will not use or disclose the UMHS's patient PHI except as permitted by the UMHS or as permitted by law.

III. POLICY STANDARDS

A. 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.

Business Associate Agreement terms and conditions are in addition to contractual language that outlines the scope of services a Business Associate is contracted to provide to the covered entity.

B. Designated Record Set

To the extent the Business Associate maintains PHI in a Designated Record Set, the Business Associate will cooperate with UMHS to honor patient rights as mandated by the Privacy Rule in accordance with the required timelines for response.

C. Authority to Execute Business Associate Agreements

Only persons authorized by this policy to do so may execute a Business Associate Agreement, and only in compliance with the provisions of this policy.

D. Covered Components Added to the Covered Entity

If a unit of U-M is added to the covered entity, the Privacy Director or his or her designee(s), with assistance from the Office of the General Counsel as necessary, 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. UMHS personnel shall forward necessary existing supplier contracts to the Privacy Director or designee for review if such contract:

- Involves the use or disclosure of UMHS PHI by the supplier; and
- Has not already been reviewed and approved by the Office of General Counsel or Privacy Director (i.e., is not a standard U-M Business Associate Agreement).
E. **New Contracts**

The general Business Associate process is illustrated below:

1. Contracts that may require Business Associate Agreements shall be routed to the appropriate processing unit/authorized signer:
   - Campus Goods and Services – University of Michigan Procurement Services
   - UMHS Goods and Services – UMHS Contracts and Procurement
   - Sponsored Research – Office of Research and Sponsored Projects (ORSP)
   - Technology Transfer – Office of Technology Transfer (OTT)
   - Offsite Clinical Professional Services, Managed Care Contracting for Clinical Services, Educational Affiliates – UMH Contracting Office
   - Agreements where UMHS has been confirmed to be a Business Associate – UMHC Contracting Office

2. All new relationships with service and product suppliers that involve the use of UMHS PHI shall be evaluated for the need of a Business Associate Agreement. This includes not only contracts with persons who will have substantial contact with such information (e.g., a business process outsourcing to a supplier for maintenance or transcription of patient records), but also those who will have only incidental contact with PHI (e.g., janitorial, security services, and certain suppliers).

3. The U-M Business Associate Agreement shall be presented to suppliers as the preferred option.
   - Purchasing may process the U-M Business Associate Agreement as long as no material changes are made.
   - Approval of the Compliance Office is required if:
     - There is any material deviation from the U-M Business Associate Agreement; or
     - The supplier’s Business Associate Agreement is used instead of the U-M Business Associate Agreement.

F. **Exceptions**

Certain parties performing activities involving UMHS PHI may be exempt from the requirement to sign a Business Associate Agreement. Consult with the Office of General Counsel and/or Privacy Director as needed. Some examples of categories of persons who may be exempt include:

- Health care providers (e.g., other physicians, hospitals, clinics, healthcare facilities, pharmacies, or ambulance companies) who receive UMHS PHI only for treatment purposes;
• Certain device manufacturers who only need PHI to counsel a surgeon on or determine the appropriate size or type of prostheses for the surgeon to use during a patient’s surgery, or otherwise assist the doctor in adjusting a device for a particular patient, in which case HIPAA treats the device manufacturer as health care provides;

• Payors who receive PHI only for payment of a claim;

• Official investigators (e.g., of the Food and Drug Administration, Centers for Medicaid and Medicare Services (CMS) or Office for Civil Rights, etc.) who receive PHI in the course of an official investigation and are not, therefore, performing a function on UMHS’ behalf (NOTE: disclosures to these agencies must be tracked);

• Certain workers who are not employed by UMHS but work mostly on site at UMHS, and who are deemed to be UMHS workforce members (these personnel are required to undergo UMHS HIPAA training and sign the UMHS Code of Conduct Attestation form.

• Certain entities participating in an Organized Health Care Arrangement with UMHS;

• Certain persons performing legally required functions or activities on behalf of UMHS, provided that UMHS shall attempt to obtain satisfactory assurances that the PHI shall be held confidential as required by 45 C.F.R. §164.504(3), and, if no such assurance is obtained, the UMHS shall document its attempts and the reason that assurances could not be obtained.

G. Disclosures to Business Associates

UMHS may disclose PHI to a Business Associate, though only as necessary to enable the Business Associate to carry out its function.

1. 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. §164.504(3). See U-M Business Associate Agreement for standard Business Associate Agreement provisions.

2. UMHS 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.

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. §164.504(3)(1). See U-M Business Associate Agreement for standard Business Associate Agreement provisions.

H. Uses and Disclosures by Business Associates

A Business Associate may use and disclose PHI only:

1. As permitted for the purposes set forth in the Business Associate Agreement;

2. For the proper management and administration of the Business Associate;
3. If expressly permitted by the terms of the Business Associate Agreement, the Business Associate may provide data aggregation services relating to UMHS’ health care operations;
4. To carry out the legal responsibilities of the Business Associate; and
5. As otherwise specified in the Business Associate Agreement.

I. Violation of Business Associate Agreements

UMHS is not required to monitor its Business Associates for compliance with their Business Associate Agreements. If UMHS 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, UMHS shall require its Business Associate to take reasonable steps to cure the breach or end the violation. If continuing violations occur, UMHS shall terminate the contract, if feasible, or if it is not feasible to terminate the agreement, and shall report the violation to the Secretary of Health and Human Services.

J. UMHS as Another Entity’s Business Associate

Where another HIPAA covered entity asserts that UMHS or UMHS personnel is their Business Associate, UMHS personnel must:

1. Obtain a written explanation from that covered entity justifying their designation of UMHS as their Business Associate; and
2. Forward the following information to the Privacy Director or designee for review:
   - The written request and justification
   - Any Business
   - A detailed description of the underlying relationship
3. Refrain from signing the agreement until they have received permission to do so from the Privacy Director or designee.

IV. PROCEDURES/ACTIONS

None

V. EXHIBITS

Business Associate Agreement Templates

- Business Associate Agreement Template (U-M as Covered Entity) - Updated May 2013
- Business Associate Agreement Template (U-M as Business Associate) - Updated May 2013

VI. REFERENCES

None
Author: UMHS Compliance Office, 615-4400

Approved provisionally by: The Health System Executive Group - April 10, 2003

Approved by:

UMHS Compliance Office - November 16, 2004
Associate Vice President, UMHS and Director and CEO, UMHHC- November 18, 2004

Reviewed by: UMHS Compliance Office with no changes required - February 2010

Reviewed and revised by UMHS Compliance Office - September 20, 2013
September 2013 revisions approved by:

UMHS Compliance Committee - September 26, 2013
Director and CEO, UMHHC - October 2, 2013
Dean, UMMS - October 16, 2013
EVPMA, UMHS - October 23, 2013

Reviewed with non-substantive revisions by UMHS Compliance Office - November 15, 2016