Business Associate Agreement

Effective Date: December 2016

Policy Statement
It is the policy of the Columbia University Healthcare Component (CUHC) to obtain a Business Associate Agreement (BAA) from a business vendor, service provider or an individual that will have access to Protected Health information (PHI).

Reason(s) for the Policy
Columbia University is required by the HIPAA Privacy and Security Rules to obtain satisfactory assurances that Protect Health Information (PHI) will be appropriately safeguarded by a business vendor, service provider or other individual that will create, receive, maintain, store or transmit Protected Health Information on behalf of the CUHC.

CUHC workforce members shall not disclose PHI to a business vendor, service provider or any other non-workforce member without a fully executed Business Associate Agreement (BAA) or other appropriate authorization.

This policy defines when a Business Associate Agreement (BAA) is required, the procedure to complete a BAA and the responsibilities for CUHC business units when a BAA is obtained.

Primary Guidance to Which This Policy Responds
HIPAA Rules 45 CFR 164.502(e), 164.504(e), 164.532(d) and (e)

Responsible University Office & Officer
Office of HIPAA Compliance, Privacy Officer

Revision History
Issued: April 2003
Revised: February 2010
November 2011
February 2013
December 2016

Who is governed by this Policy
All CUHC workforce members that will utilize a business, vendor, service provider or individual who will have access to PHI

Who Should Know This Policy
All CUHC workforce members
Exclusions & Special Situations
Researchers that may be required to disclose PHI for research purposes should follow guidance established by the Institutional Review Board (IRB).

Policy Text

1. Each vendor or service provider that create, receive, store or transmits PHI on behalf of or provide a service to the CUHC must enter into a Business Associate Agreement in which the Business Associate is obligated to protect the privacy and confidentiality of such information in accordance with the HIPAA Privacy and Security regulations.

2. A list of potential business associates include, but are not limited to the following:
   - Accreditation Organizations
   - Billing, coding and collection vendors
   - Quality Assurance Organizations
   - Consultants
   - Answering service for medical practice
   - Shredding, destruction and/or documentation storage companies
   - Medical transcription services, including contracts with an individual
   - E-prescribing gateways
   - Health Information Exchange
   - Patients satisfaction vendors
   - Personal health records
   - Data processing firms or software companies that create, receive, store or transmit PHI
   - Electronic applications
   - Law firms /attorneys
   - External auditors or accountants
   - Professional translator services
   - Software vendors

For further guidance related to a potential business associate relationship contact the Office of HIPAA Compliance.

3. Any program or business unit that establishes a business relationship meeting the definition of a Business Associate is responsible for obtaining satisfactory assurances in the form of a BAA that they will comply with the regulatory requirements to assure the confidentiality and security of the PHI.

4. Each program or business unit is responsible for identifying when a non-workforce member will create, receive, store or transmit PHI on behalf of or provide service to the CUHC and obtain a BAA.

5. Each program or business unit is responsible for maintaining a list of all active BAAs.
6. When a Business Associate relationship is terminated, it is the responsibility of the department/program or business unit to assure the return or destruction of the PHI. The department/program or business unit must also inform the Office of HIPAA Compliance when a BAA relationship is terminated.

7. All BAA’s shall be submitted to the Office of HIPAA Compliance for review and signature. The fully executed agreement is provided to the program or business unit and a copy will be maintained in the Office of HIPAA Compliance.

8. The BAA template (form) is available on the HIPAA website http://www.cumc.columbia.edu/hipaa

9. A list of all vendors, entities or individuals with a Columbia BAA is available via the HIPAA website http://www.cumc.columbia.edu/hipaa

10. If the Business Associate requests to modify the agreement or does not agree that they are acting in the capacity of Business Associate, the Office of HIPAA Compliance shall be consulted.

11. A purchase order will not be processed and access to PHI shall not be granted to the Business Associate until a BAA is fully executed.

12. Procurement will verify any agreement, contract or other business arrangement include a fully executed BAA when processing purchase orders or service agreements.

Responsibilities

- Office of HIPAA Compliance will maintain a list of all signed Business Associate agreements.
- Department Administrators will assure vendors meeting the definition of a HIPAA Business Associate have a BAA executed before permitting access to PHI.
- Procurement will verify vendors have a BAA before processing a purchase order when required and periodically verify the status of their BAA relationships.

Definitions

*Business Associate* – A person or entity that performs certain functions or activities that involve the access, use, disclosure or creation of protected health information on behalf of the Columbia University Healthcare Component.

*Columbia University Healthcare Component* – Columbia University is a Hybrid Entity that has designated as its Healthcare Component (the *Columbia University Healthcare Component*) Columbia University Medical Center and the other colleges, schools, departments and offices of the University to the extent that they (i) provide treatment or health care services and engage in Covered Transactions electronically or (ii) receive Protected Health Information to provide a service to, or perform a function for or on behalf of, the Columbia University Healthcare Component.
**Covered Entity** – (i) a health plan, (ii) healthcare clearinghouse, or (iii) healthcare provider that transmits any health information in electronic form.

**HIPAA Rules:** The HIPAA Privacy, Security Breach Notification and Enforcement Rules as amended from time to time 45 CFR 160 and 164

**Hybrid Entity** – A single legal entity (i) that is a Covered Entity (ii) whose business activities include both Covered and non-Covered functions and (iii) that designates health care components within the Hybrid Entity as more particularly described in Section 164.103

**Protected Health Information** – Information about a patient, including demographic information, that may identify a patient, which relates to the past, present, or future physical or mental health or condition of a patient; the provision of health care to a patient; or the past, present or future payment for the provision of health care to a patient.

**Contacts**
Office of HIPAA Compliance, Privacy Officer
Tel: (212) 305-7315
HIPAA@cumc.columbia.edu

**Cross References to Related Policies**
None

**Web Address**
http://www.cumc.columbia.edu/hipaa/

**Forms**

**Business Associate Agreement**

**Appendix**

**Business Associate Agreement List**
List of Business Associate Agreements

**Regulatory reference**
45 CFR § 160.103
45 CFR § 164.502(e)
45 CFR § 164.504(e)
45 CFR § 164.532(d) and (e)