Name of Standard: Business Associate Agreement Standard

Responsible Department
UMMS Office of Management (OoM)
Contact: PrivacyandCompliance@umassmed.edu or 508-856-TEAM

STANDARD STATEMENT

CWM and its Workforce perform many different roles and responsibilities for various clients, including Covered Entities. Whenever CWM creates, receives, maintains or transmits protected health information (“PHI”) to perform a function on behalf of a Covered Entity, CWM is a Business Associate under the federal HIPAA Rules. As a Business Associate, CWM recognizes its special role and responsibilities and its obligations under HIPAA Rules to safeguard the privacy and security of PHI entrusted to it by a Covered Entity¹. CWM Workforce and subcontractors must safeguard the privacy and security of PHI in performing Business Associate functions only as permitted under the HIPAA Rules and the applicable Business Associate Agreement with the Covered Entity.

REASON FOR STANDARD

The purpose of this Standard is to inform all Workforce about CWM’s role and obligations as a Business Associate when CWM performs roles and responsibilities for a Covered Entity that involve the creation, receipt, maintenance or transmission of PHI. CWM employees and contractors must safeguard the privacy and security of PHI in order to: (1) protect the privacy and security of individuals involved; (2) meet CWM contractual obligations to the Covered Entity; and (3) protect CWM from financial risks, legal liability, and reputational harm. As a Business Associate, CWM is subject to certain provisions of the HIPAA Privacy and Security Rules in the same manner as a Covered Entity, and CWM can be held directly liable for civil and criminal penalties for failure to comply with applicable portions of the HIPAA Rules.

ENTITIES AFFECTED BY THIS STANDARD

- All Business Units within CWM that perform work on behalf of a Covered Entity that involves creating, receiving, maintaining or transmitting PHI.
- All Business Units within CWM that serve as subcontractors to other organizations that delegate roles and responsibilities to CWM that involves creating, receiving, maintaining or transmitting PHI on behalf of a Covered Entity.
- Any entity with which CWM subcontracts to perform work on behalf of a Covered Entity that involves the subcontractor creating, receiving, maintaining or transmitting PHI, and for which a Business Associate Agreement is required.

¹For agreements applicable to Personally Identifiable Information not involving a Covered Entity, see the CWM Data Management Agreements Standard.
SCOPE
This Standard applies to all CWM Business Units and their employees when subcontracting work which involves creating, receiving, maintaining or transmitting PHI.

DEFINITIONS: (See Glossary on Office of Management (OoM) website for additional definitions)

RELATED DOCUMENTS
• Business Associate Agreement
• Contracts for Services Sold
• Interdepartmental Services Agreements
• Contracts for Services Purchased
• Other Agreements or Contracts Involving the Creating, Receipt, Maintenance, or Transmission of PHI On Behalf of a Covered Entity

STANDARDS
A. As a Business Associate, CWM is directly regulated under specific HIPAA Security and Privacy provisions and is directly liable for violations. In addition, CWM is subject to any additional obligations imposed under the Business Associate Agreement and must ensure that CWM subcontractors comply with these contractual obligations, as well.

1. Security: 45 CFR 164.308 (administrative safeguards); 164.310 (physical safeguards); 164.312 (technical safeguards); and 164.316 (policies and procedures and documentation requirements) of the HIPAA Security Rule apply to CWM as a Business Associate, as well as CWM subcontractors, in the same manner as such sections apply to the Covered Entity.

2. Notification: CWM as a Business Associate is obligated to notify the Covered Entity of any Breach of or Security Incident involving PHI. The Covered Entity retains the authority to determine if a Security Incident constitutes a Breach, and if a Breach requires notification to the consumer/patient. The Covered Entity shall provide the required notice, unless the Business Associate Agreement directs otherwise.

3. Privacy:
   a. As a Business Associate, CWM may use and disclose PHI only if such use and disclosure is permitted by the Covered Entity under the HIPAA Privacy Rule and the use and disclosure is not further limited under the Business Associate Agreement.
   b. CWM is not in compliance with the Privacy Rule if it knows of a violation of the Covered Entity’s obligation under the contract and fails to take steps to ensure that it is corrected.
   c. Privacy requirements that are applicable to the Covered Entity are applicable to CWM as a Business Associate and CWM subcontractors and shall be incorporated into the Business Associate Agreement.

4. Enforcement: Civil and criminal penalties may be brought directly against CWM as a Business Associate for violations of HIPAA (42 U.S.C. §1320d-5 and 6). Civil penalties may range from $100 per violation, if the Business Associate did not know and by exercising reasonable diligence would not have known of the violation, to $50,000 per
violation, if the violation was due to willful neglect and was not timely corrected, with a maximum of $1.5 million annually for identical violations. Each violation of a safeguard is a separate violation for which a penalty may be assessed, and each penalty accrues daily until corrected. In a Breach, each individual constitutes a separate violation and the violation occurs once.

B. All CWM business units entering into a Contract for Services Sold or Interdepartmental Service Agreement containing a Business Associate Agreement are responsible for reviewing the terms of the Business Associate Agreement, or other contract terms relating to privacy and security, with OoM and the UMMS Information Security Office as needed, to ensure that it can satisfactorily meet privacy and security requirements and that necessary steps are implemented prior to the effective date of the contract.

C. All CWM business units entering into a Contract for Services Purchased or other contract with a subcontractor to delegate a function, activity or service that involves PHI are responsible for reviewing the proposed contract terms (including the proposed Business Associate Agreement) with OoM and the UMMS Information Security Office, as needed, to ensure that:
   1. Applicable provisions from the Business Associate Agreement between CWM and the Covered Entity flow down to any subcontractor.
   2. CWM receives adequate and appropriate assurances from the subcontractor that it can comply with the privacy and security requirements.

D. CWM must ensure that:
   1. Workforce are appropriately trained regarding their privacy and security responsibilities, and specific requirements under the HIPAA Rules, and other state and federal laws applicable to privacy and security;
   2. All PHI received from or created on behalf of a Covered Entity or a Business Associate of a Covered Entity is kept secure, accessed only by authorized individuals, and used only for the purpose authorized under the Business Associate Agreement.

RESPONSIBILITIES
Manager of Business Unit:

1. Understand obligations of working with PHI and when a Business Associate Agreement is required and stay apprised of current developments concerning the HIPAA Rules.
2. Institute Business Unit procedures to ensure compliance with this standard and all requirements of applicable Business Associate Agreements.
3. Work collaboratively with CWM and UMMS IS to identify, educate staff on, and comply with all Business Associate Agreements or other data privacy and security contractual requirements.
4. Review all Contracts for Services Sold and Interdepartmental Service Agreements with a Covered Entity that involve creating, receiving, maintaining or transmitting PHI, for privacy and security contractual requirements, including but not limited to the Business Associate Agreement, and confer, as needed, with OoM and the UMMS Information Security Office prior to execution.
5. Review all Contracts for Services Purchased or other contracts with a subcontractor that involve creating, receiving, maintaining or transmitting PHI on behalf of a Covered Entity to ensure that all obligations imposed on CWM as a Business Associate under HIPAA Rules flow down to the subcontractor through an appropriate Business Associate
Agreement and confer, as needed, with OoM and the UMMS Information Security Office prior to execution.

**Workforce:**
1. Be responsible for knowing and following the HIPAA privacy and security obligations under the HIPAA Rules and the specific Business Associate Agreement or other contract provisions that pertain to any access to PHI.
2. Use appropriate safeguards to protect the privacy and security of the PHI in accordance with the Business Associate Agreement and the underlying contract.
3. Limit access and use of PHI to the minimum necessary for the purposes defined in the HIPAA Rules and the Business Associate Agreement or underlying contract, and for no other purposes.
4. Refer all questions about this standard to your supervisor, manager or OoM.

**Office of Management:**
1. Update as necessary the Business Associate Agreement standard form used by CWM.
2. Review, prior to signature by CWM, proposed Business Associate Agreements, Contracts for Services Sold, Contracts for Services Purchased, Interdepartmental Service Agreements, or any other contracts or agreements that involve creating, receiving, maintaining or transmitting PHI on behalf of a Covered Entity.
3. Coordinate and consult with Business Units and the UMMS Information Security Office regarding security requirements for Business Associate roles and responsibilities.
4. Serve as the compliance contact with a Covered Entity.
5. Respond to or refer, as appropriate, Workforce questions related to Business Associate roles and responsibilities.

**UMMS Information Security Office:**
1. Review Business Associate Agreements or other contract provisions that involve creating, receiving, maintaining or transmitting PHI on behalf of a Covered Entity, and work with Business Units to ensure that UMMS can comply with requirements.
2. Assist Business Units to respond to Covered Entities or other entities that request assurances that UMMS can comply with security requirements.
3. Review assurances provided by potential subcontractors to assess their ability to comply with security requirements in connection with creating, receiving, maintaining or transmitting PHI on behalf of a Covered Entity.

**VIOLATIONS**

A. All violations of this Standard shall be reported to and investigated by OoM, and other appropriate personnel, if relevant.

B. Anyone found in violation of the standards described herein may be subject to disciplinary action up to and including termination.

**DOCUMENT HISTORY**

Effective Date: 10/1/11

Revision Date(s): 2/3/12; 4/1/13; 9/23/13; 5/5/17
Review Date(s): 11/24/15; 12/1/18

APPROVAL

G.J. Campbell
Gerry Campbell
UMMS Senior Privacy Officer
Office of Management