Name of Standard: Data Management Agreements

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. In many instances, CWM is entrusted with personally identifiable information (“PII”) by a client, but CWM is not acting in the role of Business Associate under HIPAA. CWM recognizes its obligations under state and federal law to protect PII entrusted to it by its clients. CWM Workforce and subcontractors must safeguard the privacy and security of PII in performing work for clients in accordance with the applicable client agreements and state and federal law.

REASON FOR STANDARD
The purpose of this Standard is to inform all Workforce of CWM’s contractual obligations when CWM uses or receives PII to perform work for a client that is not a Covered Entity under HIPAA and therefore not subject to HIPAA requirements. CWM employees and subcontractors must safeguard PII that CWM uses or receives in our work in order to: (1) protect the privacy of the individuals for whom we maintain or process information; (2) meet our obligations to the client entity for which CWM works; and (3) protect the University from financial risks, legal liability, and reputational harm. Data Management Agreements require CWM and its subcontractors to follow practices designed to ensure the privacy and security of the PII, as required by specified state and federal laws.

ENTITIES AFFECTED BY THIS STANDARD
- All Business Units within CWM that perform work for a client that is not a Covered Entity under HIPAA and where CWM is entrusted with PII by the client.
- Any entity with which CWM subcontracts to perform work on behalf of a client that is not a Covered Entity under HIPAA, which involves the subcontractor using or receiving PII, and for which a Data Management Agreement is required.

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
- Data Management Agreement
- Contracts for Services Sold
- Interdepartmental Services Agreements

† For Business Associate requirements when UMMS is working on behalf of a HIPAA Covered Entity, see separate CWM Standard entitled “Business Associate.”
• Contracts for Services Purchased
• Other Agreements Involving the Use or Disclosure of PII

STANDARDS
A. CWM must ensure that PII entrusted to it by a client that is not a Covered Entity under HIPAA, is securely held, and only used and disclosed as authorized under the client agreement and applicable law.

B. All CWM Business Units entering into Contracts for Services Sold, or other contracts or agreements, involving the use or disclosure of PII are responsible for reviewing the 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 subcontracts (Contracts for Services Purchased) to assist CWM with commitments to its clients, which involve PII, are responsible for using the CWM Data Management Agreement standard form and reviewing the terms with OoM and the UMMS Information Security Office, as needed, to ensure that:
   1. All required terms in the client agreement with the CWM client are “pushed down” to the 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 members are appropriately trained regarding their privacy and security responsibilities, and specific requirements under the client agreement and state and federal laws.
   2. All PII received is secure, accessed only by authorized individuals, and used only for the purpose authorized under the client agreement or data management provisions.

RESPONSIBILITIES
Manager of Business Unit:
1. Understand obligations working with PII and when a Data Management Agreement is required and stay apprised of current developments concerning the privacy and security of PII.
2. Institute Business Unit procedures to ensure compliance with this standard and all requirements of applicable Data Management Agreements.
3. Work collaboratively with OoM and the UMMS Information Security Office to identify, educate staff on, and comply with all data privacy and security contractual requirements.
4. Review all Contracts for Services Sold and Interdepartmental Service Agreements for privacy and security contractual requirements, and confer, as needed, with OoM and the UMMS Information Security Office, prior to execution of such agreements.
5. Review all Contracts for Services Purchased or other contracts with subcontractors to ensure the inclusion of the CWM Data Management Agreement standard form whenever a contractor or subcontractor is expected to have access to PII.
6. Ensure that all privacy and security obligations imposed on CWM pursuant to client agreements flow to subcontractors through inclusion of appropriate terms in the CWM Data Management Agreement standard form.

Workforce:
1. Be responsible for knowing and following the privacy and security obligations under the applicable client agreement or Data Management Agreement that pertains to any access to PII.
2. Use appropriate safeguards to protect the privacy and security of the PII.
3. Limit access and use of PII to the minimum necessary for the purposes defined in the applicable client agreement or Data Management Agreement, 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 Data Management Agreement standard form used by CWM.
2. Review, prior to signature by CWM, proposed Data Management Agreements and any other contracts or agreements involving the use or disclosure of PII.
3. Coordinate and consult with UMMS IS regarding security requirements in Data Management Agreements.
4. Serve as the compliance contact with the client on communications related to PII and Data Management Agreements.
5. Respond to or refer, as appropriate, Workforce questions related to PII and Data Management Agreements.

UMMS Information Security Office:
1. Review contract provisions in Contracts for Services Sold involving the use or disclosure of PII, and work with Business Units to ensure that UMMS can comply with requirements.
2. Assist Business Units to respond to clients 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.

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 may be subject to disciplinary action up to and including termination.

DOCUMENT HISTORY

Effective Date: 4/1/13
Revision Date(s): 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