Name of Standard: Verification of Identity

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

STANDARD STATEMENT

Commonwealth Medicine (CWM) is committed to ensuring the protection of personally identifiable information (PII) in its custody and shall ensure when it is authorized to disclose PII, it is disclosed to the appropriate individual. CWM business units shall implement business unit specific procedures to ensure that prior to disclosing PII workforce members verify the identity of all individuals requesting PII, including access to or a copy of PII, if the identity of such individuals is not known.

REASON FOR STANDARD

The purpose of this standard is to provide guidance on the steps to follow to verify a requestor's identity prior to the release of PII.

ENTITIES AFFECTED BY THIS STANDARD

All Business Units and Workforce in CWM

RELATED DOCUMENTS

Use and Disclosure of PII

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

Workforce: All CWM employees (including full time, part time, long-term temporary, and probationary employees), interns, volunteers, students, and other persons whose conduct, in the performance of work for CWM, is under the direct control of CWM, whether or not the individual is paid by CWM.

SCOPE

Applies to all PII held by CWM, for which a request to release the PII is processed by CWM.

STANDARDS (Procedures)

These verification procedures are minimum standards. Business Units may establish more robust practices and may be required to follow requirements directed by their clients. Business Units also may be required to obtain permission of their respective clients prior to disclosing PII. If the Disclosure is permitted, Workforce shall, at a minimum, follow a four-step process prior to disclosing any PII:

1. **Verification of the Requestor's Authority**: If Business Unit is authorized by a client to disclose information, determine whether the individual or entity requesting the Disclosure of PII is permitted to have access to the information. Review whether the Disclosure is permissible under *Use and Disclosure of PII Standard* and Unit Specific procedures.

   For example:
   a. Is the request from the individual who is the subject of the PII?
   b. Is the request from the Personal Representative of the individual who is the subject of the PII, and is it accompanied by the appropriate documentation? or
   c. Is the request accompanied by an Authorization, and is it a valid HIPAA Authorization? (for example, the MassHealth Permission to Share Information (PSI) form).

NOTE: Requests for PII can come from various sources; all requests require careful consideration.

2. **Verification of the Requestor's Identity**: Make sure that the individual requesting the information is who he or she claims to be.
   - If the request relates to a MassHealth member, follow the MassHealth guidelines referenced below.
   - If the request relates to work for another client, be sure you follow any specific guidance provided by the client. If there is no specific direction from client follow practices outlined below.

   A. Verifying Identity by phone

   i. MassHealth members must provide their social security number (SSN) or MassHealth ID number and date of birth, which must be checked against MassHealth records.

   ii. The personal representative of a MassHealth member (including an authorized representative, appeal representative, and any others who have legal authority to act on behalf of the member, such as a parent or legal guardian) must be listed as such on MassHealth's records. The personal representative must also provide the member's MassHealth ID number and date of birth. The representative status and member information must be checked against MassHealth records.
      - If a personal representative is not designated in the MassHealth documentation, you cannot share information unless the member is also on the phone, you verify the member's identity, and the member gives permission to disclose PII to the individual during the call.
      - Authorization to share information with the representative is only good during that call unless member submits written designation to MassHealth.

   iii. A MassHealth provider must provide his or her MassHealth Provider Number, which must be checked against MassHealth records.

   iv. Other individual requestors (not MassHealth member) must provide sufficient information to demonstrate identity, for example, full name, date of birth, health insurance number or other relevant unique identifier, full or last four digits of the SSN, address, which must be checked against documentation held by program.

   v. Others to whom a disclosure is permitted without authorization, for example a DTA caseworker, must verify his or her identity by providing name, place of

employment, purpose of the disclosure, and other identifying information specific to the inquiry, such as a file or claim number.

vi. If Workforce member routinely deals with a caller and can recognize the caller's voice, he or she may confirm the caller's identity orally.

vii. If the caller/requestor cannot verify his or her identity through the above methods, do not disclose any member information of PII.

Example: *Jane Doe, a MassHealth member calls and requests that PII be shared with her daughter, who is with her at the time of the call.* If the Workforce member knows Jane Doe and can verify her voice and phone number or Jane Doe provides her MassHealth ID number and DOB and the CWM program is a program that is authorized by MassHealth to disclose information directly to the member, the Workforce member can give the information to the daughter on the phone even if the daughter is not listed on the PSI as a personal representative.

B. Verifying Identity in Person: Requests for PII may be made in person by an individual for her/his PII or an individual with an appropriate authorization may request another person's PII.

Prior to disclosing the PII, the individual's identity in both situations must be verified by:

1. MassHealth Members must present a MassHealth Card and one other form of identification*. (If they don't have their MassHealth Card, the member can provide the MassHealth ID number or SSN and date of birth, which must be checked against the MassHealth records).

2. A personal representative of a MassHealth member must provide the member's MassHealth ID number and date of birth and another form of identification* for the personal representative.

3. Other individual requestors must provide name, date of birth, unique identifier (SSN or health insurance number) or address and another form of identification. *

*Another form of identification: for example, one piece of tangible identification (preferably a photo ID) such as driver's license, employment ID badge/card, passport or other type of government issued ID.

NOTE: If an individual is requesting his/her own PII, the name on the ID provided must match the name of the individual whose PII is being sought. If the individual's name has been legally changed, evidence documenting the name change must be presented (for example, recent marriage or divorce).

C. Written Requests for PII: Since it is not possible to verify identity through the mail (US Postal or electronic) the following steps should be taken:

1. If the individual requests that PII be sent to him/her:
    a. Verify that the request is a valid. For example, does the writing match other correspondence from the member, verify that the name, address, particular information on the request is the same as those in the individual's file.
    b. If you have any question about the validity, contact the individual.

2. If the individual requests that:

a. PII be sent to another individual and encloses a valid HIPAA Authorization (including a MassHealth PSI form), verify the identity per item #1 above, and release the information only to the name and address of the individual authorized to receive the PII in accordance with the HIPAA Authorization;
b. UMMS communicate regularly with a representative on behalf of the individual, the individual client must forward a written authorization signed by the client or the representative must be listed as such on MassHealth's records.

3. If another individual requests PII (including requests by attorneys, or insurance company representatives), the requestor must include documentation of authority and a valid HIPAA authorization.

4. If the authorization form is something other than the MassHealth PSI form or a preapproved HIPAA Authorization form developed by the business unit, Workforce must validate that the authorization complies with program requirements. If there are any questions, contact OoM for assistance in determining whether the form meets requirements.

3. <u>Verification of the Record Requested</u>: Workforce members must verify that the record requested is the appropriate record. The steps taken by each Business Unit to verify the record may differ.
a. The individual's full name, date of birth, address of the individual at the date of service, or name of parents or guardians, may be used. Use the last four digits of the social security number only if there is no other information available for verification.
b. Verify that the released records include the minimum necessary to respond to the request, that they do not include information or documents beyond what was detailed in the request.

4. <u>Documentation:</u> The ID and any documentation of authority relied on shall be documented according to unit-specific methods for accounting of Disclosures (of PII).

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

RESPONSIBILITY CHART

Supervisor/manager:	Establish unit-specific verification procedures in accordance with the CWM Use and Disclosure of PII Standard and this Verification of Identity Standard. Such procedures shall be established in consultation and coordination with the verification procedures set by the client of the Business Unit.
Workforce:	Ensure that disclosing the requested PII is permitted according to unit-specific procedure. If the Disclosure is permitted, *but* the identity of a person requesting PII is not known, Workforce member shall be responsible for verifying the identity of the requestor prior to providing any PII.

DOCUMENT HISTORY

Effective Date: 10/1/11
Revision Date(s) 2/3/12, 6/1/16, 5/5/17
Review Date(s): 12/1/18, 12/1/19

APPROVAL

June Sullivan

June Sullivan
Senior Director of Compliance and Privacy
Office of Management