Verifying Identity and Authority of Persons Seeking Disclosure of a Patient’s Protected Health Information

Effective Date: April 14, 2003
Last Updated: March 26, 2020
Previously Updated: July 13, 2014
Last Reviewed: 
Next Review: 

<table>
<thead>
<tr>
<th>Functional Owner</th>
<th>UW-Madison HIPAA Privacy Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Sponsor</td>
<td>UW-Madison Chancellor</td>
</tr>
<tr>
<td>Policy Contact</td>
<td>UW-Madison HIPAA Privacy Officer</td>
</tr>
</tbody>
</table>

Policy Summary

When requests for the disclosure of protected health information are received from any person outside of the UW-Madison Health Care Component or the University of Wisconsin Affiliated Covered Entity, such individual’s identity and authority must be verified prior to making the disclosure whenever such identity and/or authority of the person is unknown to the staff person receiving the request.

Identity refers to who the person is; authority refers to the basis upon which the person claims to have access to the protected health information.

Knowledge of a requester may take the form of a known or recognized person, organization, or business, or it may be a known phone number, fax number, or mailing address.

Who This Policy Applies To

Applies to all members of the UW-Madison Health Care Component.

Rationale

In enacting HIPAA, Congress mandated the establishment of Federal standards for the privacy of individually identifiable health information. Under the patchwork of laws existing prior to adoption of HIPAA and the Privacy Rule, personal health information could be distributed—without either notice or authorization—for reasons that had nothing to do with a patient’s medical treatment or health care reimbursement. For example, unless otherwise forbidden by State or local law, without the Privacy Rule patient information held by a health plan could, without the patient’s permission, be passed on to a lender who could then deny the patient’s application for a home mortgage or a credit card, or to an employer who could use it in personnel decisions. The Privacy Rule establishes a Federal floor of safeguards to protect the confidentiality of medical information. State laws which provide stronger privacy protections apply over and above the new Federal privacy standards.
Policy Detail

1. When the Requester is the Patient

Verification of identity may be accomplished by asking for photo identification (such as a driver’s license) if the request is made in person. If the request is made over the telephone or in writing, verification may be accomplished by requesting identifying information such as address, telephone number, birth date, and/or medical record number and confirming that this information matches what is in the patient’s record.

2. When the Requester is the Patient’s Legally Authorized Representative

Verification of identity may be accomplished by asking for photo identification (such as driver’s license) if the request is made in person. Once identity is established, authority in such situations may be determined by confirming the person is named in the medical record as the person’s legally authorized representative. Or, if there is no person listed in the medical record as the patient’s legally authorized representative, authority may be established by the person presenting a copy of a valid power of attorney for health care or a copy of a court order appointing the person guardian of the person (or guardian ad litem) of the patient. If patient has no health care power of attorney and no guardian, authority may be established by following the applicable hospital or clinic policy establishing when next-of-kin becomes the legally authorized representative.

3. When the Requester is a Public Official (e.g., law enforcement officers, state or federal surveyors, medical examiners, coroners)

3.1 Identity

If the request is made in person, verification of the identity of a public official should be accomplished by the presentation of an agency identification badge, other official credentials or other proof of government status. If the request is made in writing, verification of identity will be accomplished if the request is made on the appropriate government letterhead.

3.2 Authority

Authority of the public official to have access to PHI should be established by a written statement from the public official of the legal authority under which the information is requested (or, if a written statement is impracticable, an oral statement of such authority).

Note that local law enforcement officials (e.g., city police, county sheriff) are not generally entitled to PHI without a court order or written patient authorization. There are exceptions for reporting and investigation of child abuse/neglect and for reporting gunshot wounds, certain other wounds and burns to local law enforcement officials.

When in doubt about the authority of local law enforcement officials to obtain PHI, contact with the UW-Madison Office of Legal Affairs or the UW HIPAA Privacy Officer.

3.3 Example

A police officer unknown to staff members requests PHI. The officer’s identity may be established by presentation of his/her badge and the officer’s authority to have access may be established by the officer’s written (or oral) statement of the legal authority under which the
information is requested, such as investigation of suspected child abuse (which, under state law, permits a police officer access to PHI without patient authorization).

4. Other Requesters

Procedures for verifying the identity and/or authority of other unknown requesters of PHI will vary according to the circumstances. For example, if a person who is not known or recognized presents a written authorization by the patient as the basis for obtaining PHI, the person should be requested to present identification to verify that he/she is the person named in the authorization to receive the PHI. If there are any questions concerning if and/or how to verify identity or authority in particular circumstances, contact the UW-Madison Office of Legal Affairs, the UW HIPAA Privacy Officer, or the applicable Privacy Coordinator.

Consequences for Non-Compliance

Failing to comply with this policy may result in discipline for the individual(s) responsible for such non-compliance.

Further, the US Department Health and Human Services (HHS) Office for Civil Rights (OCR) is responsible for enforcing the HIPAA Privacy and Security Rules, and an individual’s non-compliance may result in institutional non-compliance and/or an investigation by OCR. OCR attempts to resolve investigations by obtaining voluntary compliance and entering into Corrective Action Plans and Resolution Agreements. Failures to comply with HIPAA or cooperate with OCR in an investigation may result in civil and/or criminal penalties.

Supporting Tools

Additional information may be found at www.compliance.wisc.edu/hipaa

Definitions


2. Protected Health Information (“PHI”): Health information or health care payment information, including demographic information, which identifies the individual or can be used to identify the individual. PHI does not include student records held by education institutions or employment records held by employers.

3. University of Wisconsin Affiliated Covered Entity (“UW ACE”): The UW-Madison Health Care Component (except University Health Services and the State Laboratory of Hygiene), the University of Wisconsin Medical Foundation and the University of Wisconsin Hospital and Clinics. See Privacy Policy # 1.2 “Designation of UW Affiliated Covered Entity”.

4. University of Wisconsin-Madison Health Care Component (“UW HCC”): Those units of the University of Wisconsin-Madison that have been designated by the University as part of its health care component under HIPAA. See HIPAA Policy 1.1 “Designation of UW-Madison Health Care Component” for a listing of these units.
Responsibilities

HIPAA Privacy Officer
HIPAA Security Officer

Link to Current Policy

[TBD]

Link to Related Policies

https://compliance.wisc.edu/policies-and-forms/

Link to Policy History

N/A

Review / Approval

- HIPAA Executive Board, March 26, 2020