



Uses and Disclosures of PHI

Policy # 2.3

Verifying the Identity and Authority of a Person Requesting PHI

Original
Effective Date:
6/21/2016

Revised Date:
3/22/2022

Purpose: To ensure that PHI is disclosed only to people authorized to receive PHI under HIPAA rules and Federal and State medical privacy records laws.

Policy: Travis County Covered Components verify the identity and authority of the person requesting the PHI if they are not already known to the Covered Component **prior to** using or disclosing PHI as allowable by HIPAA rules and Federal and State laws.

Process:

1. When a request for PHI is made, workforce members may demand any reasonable form of identification to verify the identity of a requestor it does not already know. Acceptable forms of identification will vary, depending upon how the request is made (i.e., in person or by phone), but may include such forms and methods as are included in the chart below.

Table 1: Verification Requirements

Person Requesting PHI and Manner of Request:	Requirements for verification:
<p>Request made in person</p>	<ul style="list-style-type: none"> • A government-issued picture identification, such as a driver’s license, passport, Travis County ID, or other government issued ID with a picture. • If the requestor is a public official or is authorized by law to request PHI, workforce members can also rely on: <ol style="list-style-type: none"> 1. an agency badge, with picture; or 2. a written statement of the legal authority under which the PHI is requested
<p>Request made over the email</p>	<ul style="list-style-type: none"> • The requestor must verify the following information about the Individual whose PHI is to be disclosed: <ol style="list-style-type: none"> 1. Name 2. Address 3. Phone Number 4. Birthdate 5. Another unique identifier, such as the last four digits of the Individual’s social security number • The requestor must also give his or her name, address, and telephone number. • If the requestor is a provider, the provider should further provide the Covered Component with a copy of any authorizations or releases signed by the Individual with respect to the PHI requested. Where no release is necessary, workforce members should follow the requirements applicable to requests made in writing
<p>Request made in person by a Personal Representative</p>	<ul style="list-style-type: none"> • The requestor must have and present: <ol style="list-style-type: none"> 1. Knowledge of the Individual’s <ul style="list-style-type: none"> ○ Address ○ Phone Number ○ Birthdate ○ Another unique identifier (last 4 of SSN; email address etc...) 2. a written Power of Attorney; or 3. a signed Authorization by the individual. •The Personal Representative must also present a government-issued picture identification.

Request made in person by a Parent of a minor.	<ul style="list-style-type: none"> • If the minor is accompanied by the parent, and the minor acknowledges that the adult is his or her parent, no further information is needed. • Otherwise, the parent must follow the requirements as described in requests made in person by a personal representative.
Request made in writing	<ul style="list-style-type: none"> • Workforce members will make reasonable efforts to verify that the requestor is who he or she claims to be. This may include contacting the requestor’s employer or the Individual whose PHI is to be disclosed to discuss the request. • If the requestor is a public official, workforce members can rely on requests written on official government letterhead stationery.
Requests on behalf of a Public Official	<ul style="list-style-type: none"> • Workforce members may rely on a written statement evidencing that the person is acting on behalf of the public official

1. Workforce members examine and copy each of the documents provided and store them with the Individual’s medical records. If any questions arise about the validity of a requestor’s identity or authority, the HIPAA Compliance and Privacy Officer is consulted.
2. Once the requestor’s identity and authority are verified, workforce members determine the amount of PHI necessary to fulfill the request for disclosure. Workforce members will comply with the policy entitled [Minimum Necessary Standard](#).
3. The requested PHI is **delivered to the requesting party in a secure and confidential manner**, such that the information cannot be accessed by employees or other persons not authorized to access the PHI. If sending PHI via email, the email **must be encrypted**. You can find encrypting email instructions [here](#). To delay sending an email by putting a time and date when you would like the email sent out, you can find that [here](#).

The HIPAA Compliance and Privacy Officer or Privacy Liaison appropriately tracks the disclosure (when required; see the policy entitled [Accounting of Disclosures](#)) and delivery of the PHI.