



HIPPA Privacy Rule Policies

Policies and Procedures	Policy # 27	
VERIFICATION OF IDENTITY AND AUTHORITY		
APPROVED BY:	ADOPTED:	
	REVISED: 07122017	
SUPERCEDES POLICY: NEW	REVIEWED: 07122017	

Purpose

To describe a process for verifying the identity and authority of an individual or entity prior to disclosing Protected Health Information (PHI) to the individual or entity in accordance with state and federal privacy laws, HIPAA Regulations and LifeMed ID’s contracts with its Customers.

Policy

It is the policy of LifeMed ID to protect PHI and that LifeMed ID will verify the identity and the authority of the individual or entity prior to disclosing PHI to the individual or entity in accordance with state and federal privacy laws, HIPAA Regulations and LifeMed ID’s contracts with its customers.

All workforce members must comply with this policy. Violations of this policy will result in disciplinary action based on the seriousness of the offense or other factors. Disciplinary action may include written warning, suspension, or termination.

Definitions

“Customer” is an entity from which LifeMed ID receives PHI subject to a Business Associate Agreement (or other written agreement with the entity) in compliance with the HIPAA Regulations and approved by LifeMed ID’s legal counsel.

“Confirm” is the process of stating a fact for a person and then asking the person to assure that the fact is true. For example, a workforce member may address an individual by his/her name and then ask the individual to state his name again to guarantee the name is correct.

“Provide” is the process of giving a fact. For example, a workforce member may ask an individual to supply his/her name in order to verify identity without leading the individual to state the correct name.

For definitions of other capitalized terms or phrases, please refer to: *HIPAA-HITECH Privacy and Security Glossary*.

Procedures

1. General Rule. Prior to making a disclosure of PHI to a third party that is permitted by these Privacy Policies and Procedures, LifeMed ID’s workforce members will verify the recipient’s identity and authority to receive the PHI.





2. Reliance on Documentation. If these Policies and Procedures require any documentation, statements or representations from the intended recipient (such as a subpoena) as the basis for, or condition of, allowing a disclosure, LifeMed ID will obtain such documentation, statements or representations prior to making the disclosure.

If reasonable under the circumstances, LifeMed ID's workforce members may rely on documentation, statements or representations that, on their face, meet the requirements for disclosure. Examples of such documentation include signed Authorizations.

3. Verification of Customers Requesting PHI. LifeMed ID's workforce members will verify the identity of a customer as follows:
 - a. Written Communications: workforce members will verify that the communication is on the customer's letterhead or if an e-mail, contains the customer's domain name.
 - b. Telephone Calls: LifeMed ID's workforce members will verify the caller's identity by either personal knowledge of the customer workforce member or obtaining from the caller the following:
 - i. Customer's name,
 - ii. Individual's name,
 - iii. Individual's date of birth, and
 - iv. Caller's name and telephone number.
4. Verification of Those Requesting PHI via Phone. Before LifeMed ID's workforce members may disclose an individual's PHI on a phone call to another person or entity otherwise authorized to receive the PHI, LifeMed ID's workforce members must verify the identity of the individual or entity as follows:

- a. Individual Identification:
 - i. Outbound Calls: Minimum requirements for individual identification will be based on the individual's ability to *confirm* his or her first and last name and *provide* the following two (2) identifiers:
 - A. Date of birth, and
 - B. Address (street, city and state – exclude zip code).
 - ii. Inbound Calls: Minimum requirements for individual identification will be based on the individual's ability to *provide* the following three (3) identifiers:
 - A. First and last name,
 - B. Date of birth, and
 - C. Address (street, city and state – exclude zip code).
 - a. Caregiver/ Personal Representative Identification: Minimum requirements for verifying the identity of a Caregiver approved to discuss an individual's plan of care or an individual's Personal Representative is based on documentation in the individual's records. PHI will not be divulged to a person or persons not listed in the individual's records as Caregivers or a Personal Representative. If the Caregiver/ Personal Representative is identified in the Individual's records, LifeMed ID's workforce members will verify the identity of the Caregiver/ Personal Representative as follows:
 - i. Outbound Calls: A Caregiver must be able to *confirm* the individual's name and *provide* the following identifiers:
 - A. Individual's address,



- B. Name of self, and
- C. Relationship to individual.
- ii. Inbound Calls: A Caregiver must be able to *provide* the following identifiers:
 - A. Individual's name,
 - B. Individual's address,
 - C. Name of self, and
 - D. Relationship to individual.
- 5. Verification of Identity of Public Officials. When a government agency or public official requests PHI, LifeMed ID's workforce members may rely upon the following to verify their identity, if reliance is reasonable under the circumstances:
 - a. For in-person requests: The official's presentation of an agency identification badge, business card other official credentials or other proof of government status,
 - b. For written requests: The request, if it is on appropriate government letterhead,
 - c. For requests made by someone acting on behalf of a government official: Evidence or documentation that establishes that the person is acting on behalf of the public official, such as a written statement on appropriate government letterhead that the person is acting under the government's authority, a contract for services, a memorandum of understanding, or a purchase order.
- 6. Verification of Authority of Public Officials. When a government agency or public official requests PHI, workforce members may rely upon the following to verify their authority, if reliance is reasonable under the circumstances:
 - a. A written statement of the legal authority under which the information is requested,
 - b. If a written statement is not practical, an oral statement of the legal authority under which the information is requested, or
 - c. A copy of a warrant, subpoena, order or other Legal Process Document which is issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.
- 7. Verification of Others Requesting PHI. If LifeMed ID's workforce members receive requests from others not covered in this policy, the request will be forwarded to LifeMed ID's Privacy Office to assist in verifying identity and authority.
- 8. Inability to Verify. If LifeMed ID's workforce members are unable to verify a requestor's identity and authority, PHI will not be disclosed. The request will be forwarded to the Privacy Office to assist in verifying authority and identity.
- 9. Minimum Necessary. If the identity and authority of the party requesting PHI has been verified, LifeMed ID's workforce members may disclose PHI to the requestor but will limit the disclosure to the minimum necessary and will follow the Policies and Procedures described in *Privacy Policy #5: Minimum Necessary: Uses, Disclosures and Requests*. LifeMed ID may rely on a statement by a public official that only the minimum necessary information has been requested. Such statement must be appropriately documented.

Documentation

This version of the policy, together with any forms and other documentation created or obtained in accordance with the policy, will be retained by LifeMed ID for a period of at least 6 years plus the current year from the date of creation or the date when last in effect, whichever is later.





Regulatory Authority

45 C.F.R. §164.514 Other requirements relating to uses and disclosures of protected health

(h) **(1) Standard:** *Verification requirements. Prior to any disclosure permitted by this subpart, a covered entity must:*

(i) Except with respect to disclosures under §164.510, verify the identity of a person requesting protected health information and the authority of any such person to have access to protected health information under this subpart, if the identity or any such authority of such person is not known to the covered entity; and

(ii) Obtain any documentation, statements, or representations, whether oral or written, from the person requesting the protected health information when such documentation, statement, or representation is a condition of the disclosure under this subpart.

(2) Implementation specifications: *Verification.*

(i) Conditions on disclosures. If a disclosure is conditioned by this subpart on particular documentation, statements, or representations from the person requesting the protected health information, a covered entity may rely, if such reliance is reasonable under the circumstances, on documentation, statements, or representations that, on their face, meet the applicable requirements.

(A) The conditions in §164.512(f)(1)(ii)(C) may be satisfied by the administrative subpoena or similar process or by a separate written statement that, on its face, demonstrates that the applicable requirements have been met.

(B) The documentation required by §164.512(i)(2) may be satisfied by one or more written statements, provided that each is appropriately dated and signed in accordance with §164.512(i)(2)(i) and (v).

(ii) Identity of public officials. A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify identity when the disclosure of protected health information is to a public official or a person acting on behalf of the public official:

(A) If the request is made in person, presentation of an agency identification badge, other official credentials, or other proof of government status;

(B) If the request is in writing, the request is on the appropriate government letterhead; or

(C) If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

(iii) Authority of public officials. A covered entity may rely, if such reliance is reasonable under the circumstances, on any of the following to verify authority when the disclosure of



protected health information is to a public official or a person acting on behalf of the public official:

(A) A written statement of the legal authority under which the information is requested, or, if a written statement would be impracticable, an oral statement of such legal authority;

(B) If a request is made pursuant to legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal is presumed to constitute legal authority.

(iv) Exercise of professional judgment. The verification requirements of this paragraph are met if the covered entity relies on the exercise of professional judgment in making a use or disclosure in accordance with §164.510 or acts on a good faith belief in making a disclosure in accordance with §164.512(j).



References

Internal

1. Privacy Policy #5, Minimum Necessary; Uses, Disclosures and Requests

External

1. Omnibus Final Rule: <http://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&SID=a1031c979126e6440b522063b7bba578&rqn=div5&view=text&node=45:1.0.1.3.78&idno=45%20>