HIPPA Privacy Rule Policies

Policies and Procedures **DE-IDENTIFICATION OF HEALTH INFORMATION**	Policy # 16	
APPROVED BY: SUPERCEDES POLICY: NEW	ADOPTED:	
	REVISED: 07122017	
	REVIEWED: 07122017	

Purpose

To describe the circumstances under which LifeMed ID may create and use or provide de-identified health information in accordance with state and federal laws, HIPAA Regulations and LifeMed ID's contracts with its customer.

Policy

It is the policy of LifeMed ID to ensure that any de-identified health information used or provided on its behalf meets the requirements of this policy and is in accordance with state and federal privacy laws and HIPAA Regulations. When reasonably practical, LifeMed ID will use and provide de-identified health information, rather than Protected Health Information (PHI).

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.

See the *De-Identification Checklist* below for a description of "De-identified Health Information".

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

Procedures

1. Creation of De-Identified Health Information. To the extent permitted by applicable customer contracts, LifeMed ID may create de-identified health information from individual PHI, in accordance with this policy. LifeMed ID may allow a Subcontractor to create de-identified health information on its behalf as long as the Subcontractor has executed a Business Associate Agreement or appropriate addendum, as described in *Privacy Policy #15: Uses By and Disclosures to Subcontractors and Third Parties*. The LifeMed ID Privacy Officer is responsible for ensuring the validity of De-Identified health information that is being used or provided on a routine or non-routine basis.

2. De-Identification Procedures. PHI is deemed to be de-identified if it meets either of the following qualifications:

    a. LifeMed ID has obtained a written determination by a qualified statistician that there is very little risk that the information could be used, alone or in combination with other reasonably available information, to identify the individual. The statistician's analysis methods and results will be documented.

    b. All of the identifiers listed in the attached *De-Identification Checklist* at the end of this policy have been removed.

3. Re-Identification Codes. LifeMed ID may assign a re-identification code to de-identified health information, which is not derived from or related to information of the individual and will not be shared with any third party other than Subcontractors that have signed a Business Associate Agreement or appropriate addendum, as described in *Privacy Policy #15: Uses By and Disclosures to Subcontractors and Third Parties*.

4. Other Methods of Not Revealing Identity. In order to prevent identification of an individual's PHI when providing aggregate reports to customers, the reports must address a minimum of fifty individual participant responses. If the aggregate report contains less than fifty individual participant responses it must be sent only to the customer's Privacy Office.

5. Accounting of Disclosures. Recording of de-identified health information provided to others is not required. Any disclosure of the individual's re-identification code to a recipient of the applicable de-identified health information for purposes other than those specified as exempt from the accounting obligation set forth in *Privacy Policy #11: Accounting of Disclosures,* must be recorded in accordance with that policy.

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.

Additional Material:

De-Identification Checklist:

An individual's PHI is deemed to be de-identified if LifeMed ID does not have actual knowledge that the information could be used alone or in combination with other information to identify the individual, and all of the following elements have been removed with regard to (1) the individual, (2) the individual's relatives, (3) the individual's employer, and (4) the individual's household Individuals:

a. Names,
b. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
    i. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
    ii. The initial three (3) digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
c. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
d. Telephone numbers,
e. Fax numbers,
f. Electronic mail addresses,
g. Social security numbers,
h. Medical record numbers,
i. Health Plan or customer beneficiary numbers,
j. Account numbers,
k. Certificate/license numbers,
l. Vehicle identifiers and serial numbers,
m. Device identifiers and serial numbers,
n. Web Universal Resource Locators (URLs),
o. Internet Protocol (IP) address numbers,
p. Biometric identifiers, including finger and voice prints,
q. Full face photographic images and any comparable images, and
r. Any other unique identifying number, characteristic or code.

Regulatory Authority

45 C.F.R. §164.502 Uses and disclosures of protected health information: general rules.

(d) Standard: *Uses and disclosures of de-identified protected health information.*

(1) Uses and disclosures to create de-identified health information. A covered entity may use protected health information to create information that is not individually identifiable health information or disclose protected health information only to a business associate for such purpose, whether or not the de-identified health information is to be used by the covered entity.

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

(a) Standard: *de-identification of protected health information. that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.*

(b) Implementation specifications: *requirements for de-identification of protected health information. A covered entity may determine that health information is not individually identifiable health information only if:*

(1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:

(i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and

(ii) Documents the methods and results of the analysis that justify such determination; or

(2) (i) The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

(A) Names;

(B) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:

(1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

(2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.

(C) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

(D) Telephone numbers;

(E) Fax numbers;

(F) Electronic mail addresses;

(G) Social security numbers;

(H) Medical record numbers;

(I) Health plan beneficiary numbers;

(J) Account numbers;

(K) Certificate/license numbers;

(L) Vehicle identifiers and serial numbers, including license plate numbers;

(M) Device identifiers and serial numbers;

(N) Web Universal Resource Locators (URLs);

(O) Internet Protocol (IP) address numbers;

(P) Biometric identifiers, including finger and voice prints;

(Q) Full face photographic images and any comparable images; and

(R) Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section; and

(ii) The covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

(c) Implementation specifications: *re-identification. A covered entity may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity, provided that:*

(1) Derivation. The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and

(2) Security. The covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

References

Internal

1. Privacy Policy #11, Accounting of Disclosures
2. Privacy Policy #15, Uses and Disclosures to Subcontractors and Third Parties

External

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