



HIPPA Privacy Rule Policies

Policies and Procedures	Policy # 15	
USES BY AND DISCLOSURES TO SUBCONTRACTORS AND THIRD PARTIES		
APPROVED BY:	ADOPTED:	
	REVISED: 07122017	
SUPERCEDES POLICY: NEW	REVIEWED: 07122017	

Purpose

To describe the relationship and respective commitments, responsibilities and obligations of LifeMed ID and any Subcontractors of LifeMed ID who use or disclose Protected Health Information (PHI) on behalf of LifeMed ID 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 to require Subcontractors and other third parties who use or disclose PHI on behalf of LifeMed ID to provide satisfactory assurance that they will protect PHI which will be documented through a written Business Associate Agreement (BAA) or other agreement that meets the requirements of 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

“Business Associate” - See the definition of “business associate” in the Regulatory Authority section of this Policy.

“Business Associate Agreement” or “BAA” means an agreement between a Covered Entity and its Business Associate (or a Business Associate and its vendor or subcontractor) in which the Business Associate (or a Business Associate’s vendor or subcontractor, as the case may be) agrees to restrict its use and disclosure of Protected Health Information and meets the requirements of 45 C.F.R. §164.504(e).

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

“Subcontractor” includes any Business Associate, person or entity (e.g. vendor or subcontractor) that creates, receives, maintains, transmits or otherwise has access to PHI on a routine basis in connection with the fulfillment of LifeMed ID ’s obligations under its BAA with its customer.





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

Procedures

1. Identify Subcontractors. LifeMed ID's designated contracting officer, in conjunction with the Privacy Officer, will identify all of its Subcontractors that handle PHI. A Subcontractor does not include persons or entities that would not, in the normal course of their activities, use or disclose PHI but who may inadvertently come into contact with such information. LifeMed ID's designated contracting office, in conjunction with the Privacy Officer, will ensure that those persons or entities sign a confidentiality agreement but are otherwise not covered by this policy.
2. Disclosures to Subcontractors. The contractual requirements of the Privacy Rule apply to any contract or other arrangement between LifeMed ID and its Subcontractors in the same manner as such requirements apply to contracts or other arrangements between a Covered Entity and a Business Associate. LifeMed ID may disclose PHI to a Subcontractor and may allow the Subcontractor to create, receive, maintain, or transmit PHI on its behalf, if LifeMed ID obtains satisfactory assurances, in accordance with contractual requirements outlined in the HIPAA Privacy Rule, that the Subcontractor will appropriately safeguard the PHI.
3. Subcontractor Agreements. All BAAs with Subcontractors will be reviewed, approved, including legal approval, and signed under the LifeMed ID's policies and procedures for contracting, procurement and/or sourcing. LifeMed ID's designated contracting officer, in collaboration with the Privacy Officer and legal counsel, will ensure the following:
 - a. All BAAs with Subcontractors covered by this policy will include appropriate language regarding LifeMed ID's duties and obligations as a Business Associate of its customers.
 - b. Whenever possible, the attached form entitled *SAMPLE BUSINESS ASSOCIATE AGREEMENT PROVISIONS* provided by DHHS should be used if LifeMed ID does not have a separate written service agreement with Subcontractors. Exceptions require consultation with the LifeMed ID's legal counsel.
 - c. LifeMed ID's legal counsel must be consulted if the Subcontractor wishes to add or change any of the terms, to ensure that the changes meet legal and regulatory requirements and do not adversely affect LifeMed ID. If the Subcontractor offers its own form of BAA, the BAA must adequately cover all of the requirements set forth in LifeMed ID's form of BAA or in the attached *SAMPLE BUSINESS ASSOCIATE AGREEMENT PROVISIONS* and legal counsel will be consulted to ensure that it does not include other elements or provisions that do not meet legal and regulatory requirements or that could adversely affect LifeMed ID.
4. Subcontractor's Obligations under the BAA. Prior to entering into a BAA, the Subcontractor must be able to demonstrate to LifeMed ID's Privacy Officer that it has policies and procedures in place to ensure that it will adequately safeguard PHI. The terms of the BAA will:



- a. Establish the permitted and required uses and disclosures of PHI by the Subcontractor; the BAA may not authorize the use or further disclosure of PHI in a manner that would violate the HIPAA Privacy Rule if done by LifeMed ID except that:
 - i. The BAA may permit the Subcontractor to use and disclose PHI for the proper management and administration of its affairs, and
 - ii. The BAA may permit the Subcontractor to provide Data Aggregation services relating to the Health Care Operations of LifeMed ID.

- b. Provide that the Subcontractor will:
 - i. Not use or further disclose the PHI other than as permitted or required by the BAA or as required by law,
 - ii. Use appropriate safeguards and comply, where applicable, with the HIPAA Security Rule with respect to electronic PHI to prevent use or disclosure of the information other than as provided for by its BAA,
 - iii. Report to LifeMed ID any use or disclosure of PHI not provided for by its BAA of which it becomes aware, including breaches of unsecured PHI,
 - iv. Ensure that any of its Subcontractors (e.g. vendors and subcontractors of the Subcontractor) that create, receive, maintain, or transmit PHI on behalf of the Subcontractor agree to the same restrictions and conditions that apply to the Subcontractor with respect to such PHI,
 - v. To the extent the Subcontractor is to carry out LifeMed ID's obligation under the HIPAA Privacy Rule, comply with those regulations that apply to LifeMed ID in the performance of such obligation,
 - vi. Make its internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by the Subcontractor on behalf of LifeMed ID, available to the Secretary of the Department of Health and Human Services for purposes of determining compliance with the HIPAA Privacy Rule,
 - vii. Provide that, at the termination of the BAA, the Subcontractor will, if feasible, return or destroy PHI received, created or maintained by the Subcontractor from or on behalf of LifeMed ID; if such return or destruction is not feasible, it will agree to extend the protections of the BAA to the PHI and limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible,
 - viii. Authorize termination of a BAA by the Subcontractor if it determines that its Subcontractor has violated a material term of the BAA, and



- c. Require the Subcontractor to assist LifeMed ID in a timely manner if a request for PHI is received, including investigating the validity of the request and, if valid:
 - i. Providing the individual with copies or access to the PHI upon the request of LifeMed ID,
 - ii. Amending the information upon request from LifeMed ID,
 - iii. Maintaining an Accounting of all Disclosures for purposes other than Treatment and Payment purposes or Health Care Operations or other purposes excluded from the accounting obligation, and provide the accounting to LifeMed ID upon request. Refer to: *Privacy Policy #11: Accounting of Disclosures*, and
 - iv. Complying with all LifeMed ID's requests regarding confidential communications and restrictions on the use and disclosure of PHI. Refer to: *Privacy Policy #7: Requests for Restrictions of Uses and Disclosures* and *Privacy Policy #8: Requests for Confidential Communications*.
 - d. The Subcontractor must be able to assist LifeMed ID in a timely manner if LifeMed ID's customer requests or seeks information related to PHI.
5. Notification to Subcontractors. The LifeMed ID's Privacy Officer will, if appropriate:
- a. Provide the Subcontractors with copies of the Notice of Privacy Practices of the customer,
 - b. Notify its Subcontractors when it becomes aware that a customer has changed its Notice of Privacy Practices in a manner that affects the Subcontractors, and
 - c. Document the name of the person notified as well as the date(s) when the Subcontractor was initially notified and when notified of any change.
6. Minimum Necessary Disclosures. All disclosures to Subcontractors will be limited to the minimum amount of information needed for the Subcontractor to carry out its functions on behalf of LifeMed ID. Subcontractors are subject to the same "minimum necessary" limitations as LifeMed ID, as outlined in *Privacy Policy #5: Minimum Necessary: Uses, Disclosures and Requests*.
7. Violations by Subcontractors.
- a. Any LifeMed ID workforce member who learns, or has reason to believe, that a Subcontractor is in any way jeopardizing the privacy and confidentiality of PHI provided by LifeMed ID, will notify LifeMed ID's Privacy Officer immediately.
 - b. LifeMed ID's Privacy Officer will notify the Subcontractor immediately to cease such activities and will work with the Subcontractor on mitigating any harmful effect that may result from the violation.



- c. If the violation is not remedied with the Subcontractor, the BAA with the Subcontractor may be terminated. If permitted by the applicable customer contract, the Privacy Officer, in consultation with legal counsel, may determine if a reasonable cure period may be allowed.
 - d. If termination is not feasible because the Subcontractor is the only qualified and available person or entity for such services, the LifeMed ID Privacy Officer will inform the customer's Privacy Office of the reason for no termination and will appropriately document the reason for no termination.
 - e. LifeMed ID's Privacy Officer will notify the customer's Privacy Office of the violation within the time period specified in LifeMed ID's contract with the customer.
8. Termination of Subcontractor Agreement. If the BAA with your Subcontractor is terminated for any reason, LifeMed ID will stop disclosing any PHI to the Subcontractor and require the Subcontractor to do the following:
 - a. Return all PHI in its possession or ensure that the PHI is properly destroyed in a manner that protects the confidentiality of the PHI. The Subcontractor will be required to provide a certificate of destruction showing that the PHI has been properly destroyed.
 - b. If any of the PHI cannot be returned or destroyed (for example, because the Subcontractor is required to maintain certain information for inspection by regulatory agencies), the Subcontractor may retain the PHI as long as it continues to protect the PHI in accordance with the terms of the BAA and to use the information only for the purposes that make return or destruction infeasible.
9. Accounting of Disclosures to Subcontractors. It is not necessary to include disclosures to LifeMed ID's Subcontractors in an Accounting of Disclosures. However, Subcontractors are required to maintain a record of their disclosures to the same extent as LifeMed ID is required to do so. Refer to: *Privacy Policy #11: Accounting of Disclosures.*
10. Uses and Disclosures to Third Parties for Certain Legal Responsibilities, Management and Administration.
 - a. When permitted by the applicable customer contract(s), LifeMed ID's Privacy Officer may approve the disclosure of PHI to third parties for purposes of LifeMed ID's fulfillment of legal responsibilities, management and administration.
 - b. In such instances, contracts must be executed with the third party containing at least the following: (i) an obligation to hold the PHI confidentially and use it or further disclose it only as required by law or for the purpose for which it was disclosed; and (ii) an obligation to notify the LifeMed ID's Privacy Officer of any instances in which the confidentiality of the PHI has been compromised.



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. §160.103 Definitions.

Business associate:

(1) Except as provided in paragraph (4) of this definition, business associate means a person who is not a member of the covered entity's workforce and who:

(i) On behalf of a covered entity, creates, receives, maintains, or transmits protected health information for a function or activity regulated by the Privacy Rule, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, patient safety activities, billing, benefit management, practice management, and repricing; or

(ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 164.504(f) of this subchapter apply and are met.

(iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.

(2) A covered entity may be a business associate of another covered entity.

(3) Business associate includes:

(i) A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires access on a routine basis to such protected health information.

(ii) A person that offers a personal health record to one or more individuals on behalf of a covered entity.

(iii) A subcontractor that creates, receives, maintains, or transmits protected health information on behalf of the business associate.

(4) Business associate does not include:

(i) A health care provider, with respect to disclosures by a covered entity to the health care provider concerning the treatment of the individual.

(ii) A plan sponsor, with respect to disclosures by a group health plan (or by a health insurance issuer or HMO with respect to a group health plan) to the plan sponsor, to the extent that the requirements of § 164.504(f) of this subchapter apply and are met.

(iii) A government agency, with respect to determining eligibility for, or enrollment in, a government health plan that provides public benefits and is administered by another



government agency, or collecting protected health information for such purposes, to the extent such activities are authorized by law.

45 C.F.R. §164.500 Applicability.

(a) Except as otherwise provided herein, the standards, requirements, and implementation specifications of this subpart apply to covered entities with respect to protected health information.

(c) Where provided, the standards, requirements, and implementation specifications adopted under this subpart apply to a business associate with respect to the protected health information of a covered entity.

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

(a) **Standard.** A covered entity or business associate may not use or disclose protected health information, except as permitted or required by this subpart or by subpart C of part 160 of this subchapter.

(3) *Business associates: Permitted uses and disclosures.* A business associate may use or disclose protected health information only as permitted or required by its business associate contract or other arrangement pursuant to § 164.504(e) or as required by law. The business associate may not use or disclose protected health information in a manner that would violate the requirements of this subpart, if done by the covered entity, except for the purposes specified under § 164.504(e)(2)(i)(A) or (B) if such uses or disclosures are permitted by its contract or other arrangement.

(4) *Business associates: Required uses and disclosures.* A business associate is required to disclose protected health information:

(i) When required by the Secretary under subpart C of part 160 of this subchapter to investigate or determine the business associate's compliance with this subchapter.

(ii) To the covered entity, individual, or individual's designee, as necessary to satisfy a covered entity's obligations under § 164.524(c)(2)(ii) and (3)(ii) with respect to an individual's request for an electronic copy of protected health information.

(5) *Prohibited uses and disclosures.*

(ii) *Sale of protected health information:*

(A) Except pursuant to and in compliance with § 164.508(a)(4), a covered entity or business associate may not sell protected health information.

(B) For purposes of this paragraph, sale of protected health information means:

(2) Sale of protected health information does not include a disclosure of protected health information:

(v) To or by a business associate for activities that the business associate undertakes on behalf of a covered entity, or on behalf of a business associate in the case of a subcontractor, pursuant to §§ 164.502(e) and



164.504(e), and the only remuneration provided is by the covered entity to the business associate, or by the business associate to the subcontractor, if applicable, for the performance of such activities;

(b) Standard: *Minimum necessary*

(1) Minimum necessary applies. When using or disclosing protected health information or when requesting protected health information from another covered entity or business associate, a covered entity or business associate must make reasonable efforts to limit protected health information to the minimum necessary to accomplish the intended purpose of the use, disclosure, or request.

(e) (1) Standard: *Disclosures to business associates.*

(i) A covered entity may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain, or transmit protected health information on its behalf, if the covered entity obtains satisfactory assurance that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.

(ii) A business associate may disclose protected health information to a business associate that is a subcontractor and may allow the subcontractor to create, receive, maintain, or transmit protected health information on its behalf, if the business associate obtains satisfactory assurances, in accordance with § 164.504(e)(1)(i), that the subcontractor will appropriately safeguard the information.

(2) Implementation specification: Documentation. The satisfactory assurances required by paragraph (e)(1) of this section must be documented through a written contract or other written agreement or arrangement with the business associate that meets the applicable requirements of §164.504(e).

45 C.F.R. § 164.504 Uses and disclosures: Organizational requirements.

(e) (1) Standard: *Business associate contracts.*

(i) The contract or other arrangement required by §164.502(e)(2) must meet the requirements of paragraph (e)(2), (e)(3) or (e)(5) of this section, as applicable.

(ii) A covered entity is not in compliance with the standards in §164.502(e) and this paragraph, if the covered entity knew of a pattern of activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

(iii) A business associate is not in compliance with the standards in § 164.502(e) and this paragraph, if the business associate knew of a pattern of activity or practice of a



subcontractor that constituted a material breach or violation of the subcontractor's obligation under the contract or other arrangement, unless the business associate took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful, terminated the contract or arrangement, if feasible.

(2) Implementation specifications: *Business associate contracts. A contract between the covered entity and a business associate must:*

(i) Establish the permitted and required uses and disclosures of protected health information by the business associate. The contract may not authorize the business associate to use or further disclose the information in a manner that would violate the requirements of this subpart, if done by the covered entity, except that:

(A) The contract may permit the business associate to use and disclose protected health information for the proper management and administration of the business associate, as provided in paragraph (e)(4) of this section; and

(B) The contract may permit the business associate to provide data aggregation services relating to the health care operations of the covered entity.

(ii) Provide that the business associate will:

(A) Not use or further disclose the information other than as permitted or required by the contract or as required by law;

(B) Use appropriate safeguards and comply, where applicable, with subpart C of this part with respect to electronic protected health information, to prevent use or disclosure of the information other than as provided for by its contract;

(C) Report to the covered entity any use or disclosure of the information not provided for by its contract of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410;

(D) In accordance with § 164.502(e)(1)(ii), ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the business associate agree to the same restrictions and conditions that apply to the business associate with respect to such information;

(E) Make available protected health information in accordance with §164.524;

(F) Make available protected health information for amendment and incorporate any amendments to protected health information in accordance with §164.526;

(G) Make available the information required to provide an accounting of disclosures in accordance with §164.528;

(H) To the extent the business associate is to carry out a covered entity's obligation under this subpart, comply with the regulations of this subpart that apply to the covered entity in the performance of such obligation.



(I) Make its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity available to the Secretary for purposes of determining the covered entity's compliance with this subpart; and

(J) At termination of the contract, if feasible, return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity that the business associate still maintains in any form and retain no copies of such information or, if such return or destruction is not feasible, extend the protections of the contract to the information and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

(iii) Authorize termination of the contract by the covered entity, if the covered entity determines that the business associate has violated a material term of the contract. [see exception (3)(iii)]

(3) Implementation specifications: Other arrangements.

(i) If a covered entity and its business associate are both governmental entities:

(A) The covered entity may comply with this paragraph and § 164.314(a)(1), if applicable, by entering into a memorandum of understanding with the business associate that contains terms that accomplish the objectives of paragraph (e)(2) of this section and § 164.314(a)(2), if applicable.

(B) The covered entity may comply with this paragraph and § 164.314(a)(1), if applicable, if other law (including regulations adopted by the covered entity or its business associate) contains requirements applicable to the business associate that accomplish the objectives of paragraph (e)(2) of this section and § 164.314(a)(2), if applicable.

(ii) If a business associate is required by law to perform a function or activity on behalf of a covered entity or to provide a service described in the definition of business associate in §160.103 of this subchapter to a covered entity, such covered entity may disclose protected health information to the business associate to the extent necessary to comply with the legal mandate without meeting the requirements of this paragraph and § 164.314(a)(1), if applicable, provided that the covered entity attempts in good faith to obtain satisfactory assurances as required by paragraph (e)(2) of this section and § 164.314(a)(1), if applicable, and, if such attempt fails, documents the attempt and the reasons that such assurances cannot be obtained.

(iii) The covered entity may omit from its other arrangements the termination authorization required by paragraph (e)(2)(iii) of this section, if such authorization is inconsistent with the statutory obligations of the covered entity or its business associate.

(iv) A covered entity may comply with this paragraph and § 164.314(a)(1) if the covered entity discloses only a limited data set to a business associate for the business associate to carry out a health care operations function and the covered entity has a data use



agreement with the business associate that complies with § 164.514(e)(4) and § 164.314(a)(1), if applicable.

(4) Implementation specifications: *Other requirements for contracts and other arrangements.*

(i) The contract or other arrangement between the covered entity and the business associate may permit the business associate to use the information received by the business associate in its capacity as a business associate to the covered entity, if necessary:

(A) For the proper management and administration of the business associate; or

(B) To carry out the legal responsibilities of the business associate.

(ii) The contract or other arrangement between the covered entity and the business associate may permit the business associate to disclose the information received by the business associate in its capacity as a business associate for the purposes described in paragraph (e)(4)(i) of this section, if:

(A) The disclosure is required by law; or

(B)(1) The business associate obtains reasonable assurances from the person to whom the information is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person; and

(2) The person notifies the business associate of any instances of which it is aware in which the confidentiality of the information has been breached.

(5) Implementation specifications: *Business associate contracts with subcontractors. The requirements of § 164.504(e)(2) through (e)(4) apply to the contract or other arrangement required by § 164.502(e)(1)(ii) between a business associate and a business associate that is a subcontractor in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.*

Other Situations in Which a Business Associate Contract Is NOT Required.

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/businessassociates.html>

- 1. When a health care provider discloses protected health information to a health plan for payment purposes, or when the health care provider simply accepts a discounted rate to participate in the health plan's network. A provider that submits a claim to a health plan and a health plan that assesses and pays the claim are each acting on its own behalf as a covered entity, and not as the "business associate" of the other.*
- 2. With persons or organizations (e.g., janitorial service or electrician) whose functions or services do not involve the use or disclosure of protected health information, and where any access to protected health information by such persons would be incidental, if at all.*



3. *With a person or organization that acts merely as a conduit for protected health information, for example, the US Postal Service, certain private couriers, and their electronic equivalents. Among covered entities who participate in an organized health care arrangement (OHCA) to make disclosures that relate to the joint health care activities of the OHCA.*
4. *Where a group health plan purchases insurance from a health insurance issuer or HMO. The relationship between the group health plan and the health insurance issuer or HMO is defined by the Privacy Rule as an OHCA, with respect to the individuals they jointly serve or have served. Thus, these covered entities are permitted to share protected health information that relates to the joint health care activities of the OHCA.*
5. *Where one covered entity purchases a health plan product or other insurance, for example, reinsurance, from an insurer. Each entity is acting on its own behalf when the covered entity purchases the insurance benefits, and when the covered entity submits a claim to the insurer and the insurer pays the claim.*
6. *To disclose protected health information to a researcher for research purposes, either with patient authorization, pursuant to a waiver under 45 CFR 164.512(i), or as a limited data set pursuant to 45 CFR 164.514(e). Because the researcher is not conducting a function or activity regulated by the Administrative Simplification Rules, such as payment or health care operations, or providing one of the services listed in the definition of "business associate" at 45 CFR 160.103, the researcher is not a business associate of the covered entity, and no business associate agreement is required.*
7. *When a financial institution processes consumer-conducted financial transactions by debit, credit, or other payment card, clears checks, initiates or processes electronic funds transfers, or conducts any other activity that directly facilitates or affects the transfer of funds for payment for health care or health plan premiums. When it conducts these activities, the financial institution is providing its normal banking or other financial transaction services to its customers; it is not performing a function or activity for, or on behalf of, the covered entity.*

45 C.F.R. §164.532 Transition provisions.

(a) Standard: *Effect of prior authorizations. Notwithstanding §§164.508 and 164.512(i), a covered entity may use or disclose protected health information, consistent with paragraphs (b) and (c) of this section, pursuant to an authorization or other express legal permission obtained from an individual permitting the use or disclosure of protected health information, informed consent of the individual to participate in research, or a waiver of informed consent by an IRB, or a waiver of authorization in accordance with §164.512(i)(1)(i) .*

(b) Implementation specification: *Effect of prior authorization for purposes other than research. Notwithstanding any provisions in §164.508, a covered entity may use or disclose protected health information that it created or received prior to the applicable compliance date of this subpart pursuant to an authorization or other express legal permission obtained from an individual prior to the applicable compliance date of this subpart, provided that the authorization or other express legal permission specifically permits such use or disclosure and there is no agreed-to restriction in accordance with §164.522(a).*

(c) Implementation specification: *Effect of prior permission for research. Notwithstanding any provisions in §§164.508 and 164.512(i), a covered entity may, to the extent allowed by one of the following permissions,*





use or disclose, for research, protected health information that it created or received either before or after the applicable compliance date of this subpart, provided that there is no agreed-to restriction in accordance with §164.522(a), and the covered entity has obtained, prior to the applicable compliance date, either:

- (1) An authorization or other express legal permission from an individual to use or disclose protected health information for the research;
- (2) The informed consent of the individual to participate in the research; or
- (3) A waiver, by an IRB, of informed consent for the research, in accordance with 7 CFR 1c.116(d), 10 CFR 745.116(d), 14 CFR 1230.116(d), 15 CFR 27.116(d), 16 CFR 1028.116(d), 21 CFR 50.24, 22 CFR 225.116(d), 24 CFR 60.116(d), 28 CFR 46.116(d), 32 CFR 219.116(d), 34 CFR 97.116(d), 38 CFR 16.116(d), 40 CFR 26.116(d), 45 CFR 46.116(d), 45 CFR 690.116(d), or 49 CFR 11.116(d), provided that a covered entity must obtain authorization in accordance with §164.508 if, after the compliance date, informed consent is sought from an individual participating in the research; or
- (4) A waiver of authorization in accordance with §164.512(i)(1)(i).

(d) Standard: *Effect of prior contracts or other arrangements with business associates. Notwithstanding any other provisions of this subpart, a covered entity or business associate with respect to a subcontractor, may disclose protected health information to a business associate and may allow a business associate to create, receive, maintain or transmit protected health information on its behalf pursuant to a written contract or other written arrangement with such business associate that does not comply with §§164.308(b), 164.314(a), 164.502(e) and 164.504(e) only in accordance with paragraph (e) of this section.*

(e) Implementation specification: *Deemed compliance*

(1) *Qualification. Notwithstanding other sections of this part, a covered entity, or business associate with respect to a subcontractor, is deemed to be in compliance with the documentation and contract requirements of §§164.308(b), 164.314(a), 164.502(e) and 164.504(e), with respect to a particular business associate relationship, for the time period set forth in paragraph (e)(2) of this section, if:*

- (i) *Prior to January 25, 2013, such covered entity, or business associate with respect to a subcontractor, has entered into and is operating pursuant to a written contract or other written arrangement with the business associate that complies with the applicable provisions of §§ 164.314(a) or 164.504(e) that were in effect on such date; and*
- (ii) *The contract or other arrangement is not renewed or modified from March 26, 2013, until September 23, 2013.*

(2) *Limited deemed compliance period. A prior contract or other arrangement that meets the qualification requirements in paragraph (e) of this section shall be deemed compliant until the earlier of:*

- (i) *The date such contract or other arrangement is renewed or modified on or after September 23, 2013; or*
- (ii) *September 22, 2014.*



(3) Covered entity responsibilities. Nothing in this section shall alter the requirements of a covered entity to comply with part 160, subpart C of this subchapter and §§164.524, 164.526, 164.528, and 164.530(f) with respect to protected health information held by a business associate.

(f) Effect of prior data use agreements. If, prior to [January 25, 2013, a covered entity has entered into and is operating pursuant to a data use agreement with a recipient of a limited data set that complies with § 164.514(e), notwithstanding § 164.502(a)(5)(ii), the covered entity may continue to disclose a limited data set pursuant to such agreement in exchange for remuneration from or on behalf of the recipient of the protected health information until the earlier of: (1) The date such agreement is renewed or modified on or after September 23, 2013; or (2) September 22, 2014.

<http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/contractprov.html>



HIPAA Business Associate Agreement

This Business Associate Agreement ("**Agreement**") effective on **xxx, 2016** ("**Effective Date**") is entered into by and between _____ (the "**Covered Entity**") and LifeMed ID, Inc. 6349 Auburn Blvd. Citrus Heights CA 95621 (the "**Business Associate**").

RECITALS:

A. The purpose of this Agreement is to comply with the Standards for Privacy and Security of Individually Identifiable Health Information ("protected health information") issued by the Secretary of the U.S. Department of Health and Human Services ("HHS") 45 C.F.R. Part 160 and Part 164 (the "Privacy and Security Regulation") under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and Title XIII, The Health Information Technology for Economic and Clinical Health Act ("HITECH"), of the American Recovery and Reinvestment Act ("ARRA").

B. Covered Entity requests Business Associate to perform services for it which may include protected health information subject to the condition that Business Associate agrees to abide by the requirements set forth in the Privacy and Security Regulation and HITECH.

C. This Agreement sets forth the terms and conditions pursuant to which protected health information that is provided by, or created or received by, the Business Associate from or on behalf of the Covered Entity will be handled and shall supersede and replace any prior Business Associate Agreement between the parties.

NOW, THEREFORE, in consideration of the foregoing and of the mutual covenants and agreements hereinafter addressed, the parties agree as follows:

Services. The Business Associate provides services for the Covered Entity that can involve the use and disclosure of protected health information. Except as otherwise specified herein, the Business Associate may make any and all uses of protected health information necessary to perform the services requested by the Covered Entity. Additionally, Business Associate may disclose protected health information for the purposes authorized by this Agreement only to its employees, subcontractors and agents as directed by the Covered Entity.

Obligations and Activities of Business Associate. With regard to its use and/or disclosure of protected health information, the Business Associate hereby agrees to:

- (a) Not use or disclose protected health information other than as permitted or required by the Agreement or as required by law





(b) Use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information to prevent use or disclosure of protected health information other than as provided for by the Agreement

(c) Report to Covered Entity any use or disclosure of protected health information not provided for by the Agreement of which it becomes aware, including breaches of unsecured protected health information as required at 45 CFR 164.410, and any security incident of which it becomes aware

(d) In accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any subcontractors that create, receive, maintain, or transmit protected health information on behalf of the Business Associate agree to the same restrictions, conditions, and requirements that apply to the Business Associate with respect to such information

(e) Make available protected health information in a designated record set to the Covered Entity as necessary to satisfy Covered Entity's obligations under 45 CFR 164.524

(f) Make any amendment(s) to protected health information in a designated record set as directed or agreed to by the Covered Entity pursuant to 45 CFR 164.526, or take other measures as necessary to satisfy Covered Entity's obligations under 45 CFR 164.526

(g) Maintain and make available the information required to provide an accounting of disclosures to the Covered Entity as necessary to satisfy Covered Entity's obligations under 45 CFR 164.528

(h) To the extent the Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s)

(i) Make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules

Permitted Uses and Disclosures by Business Associate

(a) Business Associate may only use or disclose protected health information

(b) Business Associate may use or disclose protected health information as required by law

(c) Business Associate agrees to make uses and disclosures and requests for protected health information

(d) Business Associate may not use or disclose protected health information in a manner that would violate Subpart E of 45 CFR Part 164 if done by Covered Entity

Provisions for Covered Entity to Inform Business Associate of Privacy Practices and Restrictions





(a) Covered Entity shall notify Business Associate of any limitation(s) in the notice of privacy practices of Covered Entity under 45 CFR 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of protected health information.

(b) Covered Entity shall notify Business Associate of any changes in, or revocation of, the permission by an individual to use or disclose his or her protected health information, to the extent that such changes may affect Business Associate's use or disclosure of protected health information.

(c) Covered Entity shall notify Business Associate of any restriction on the use or disclosure of protected health information that Covered Entity has agreed to or is required to abide by under 45 CFR 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of protected health information

Permissible Requests by Covered Entity

Covered Entity shall not request Business Associate to use or disclose protected health information in any manner that would not be permissible under Subpart E of 45 CFR Part 164 if done by Covered Entity.

Term and Termination

(a) Term. The Term of this Agreement shall be effective as of the Effective Date and shall continue in effect until all requested services and obligations of the parties have been met, unless terminated as provided herein or by mutual agreement of the parties.

(b) Termination for Cause. Business Associate authorizes termination of this Agreement by Covered Entity, if Covered Entity determines Business Associate has violated a material term of the Agreement and Business Associate has not cured the breach or ended the violation within 10 days following written notice of the existence of an alleged material breach. Covered Entity will afford the Business Associate an opportunity to cure said alleged material breach upon mutually agreeable terms. Failure to cure in the manner set forth in this paragraph is grounds for the immediate termination of the Agreement. If termination is not feasible, the Covered Entity shall report the breach to the Secretary of HHS.

(c) Obligations of Business Associate Upon Termination. Upon termination of this Agreement for any reason, Business Associate shall return to Covered Entity or, if agreed to by Covered Entity, destroy all protected health information received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, that the Business Associate still maintains in any form. Business Associate shall retain no copies of the protected health information.



Upon termination of this Agreement for any reason, Business Associate, with respect to protected health information received from Covered Entity, or created, maintained, or received by Business Associate on behalf of Covered Entity, shall:

1. Retain only that protected health information which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities
2. Return to Covered Entity or, if agreed to by Covered Entity, destroy the remaining protected health information that the Business Associate still maintains in any form
3. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to electronic protected health information to prevent use or disclosure of the protected health information, other than as provided for in this Section, for as long as Business Associate retains the protected health information
4. Not use or disclose the protected health information retained by Business Associate other than for the purposes for which such protected health information was retained and subject to the same conditions set out under section titled “Permitted Uses and Disclosures By Business Associate” which applied prior to termination
5. Return to Covered Entity or, if agreed to by Covered Entity, destroy the protected health information retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities

(d) Survival. The obligations and rights of Business Associate and Covered Entity under this Section shall survive the termination of this Agreement indefinitely.

Mutual Representation and Warranty. Each party represents and warrants to the other party that all of its employees, agents, representatives and members of its work force, whose services may be used to fulfill obligations under this Agreement, are or shall be appropriately informed of the terms of this Agreement and are obligated to comply with all provisions of this Agreement.

Amendment. This Agreement may not be modified or amended, except in writing as agreed to by each party. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of the Privacy and Security Regulation, HITECH Act and subsequent additions or amendments related to such laws.

No Third Party Beneficiaries. Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer, upon any person other than the parties hereto any rights, remedies, obligations, or liabilities whatsoever.



Notices. Any notices to be given hereunder shall be made via U.S. mail or express courier, or hand delivery to the other party's address given below as follows:

If to Covered Entity: Name

Address: Address

If to Business Associate: LifeMed ID, Inc.

Address: 6349 Auburn Blvd., Citrus Heights, CA 95621

10. Interpretation. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with the Privacy and Security Rule.

IN WITNESS WHEREOF, the parties hereto hereby set their hands and seals as of the th day of xxx, 20.

COVERED ENTITY -

Sig: _____

Name: _____

Title: _____

Date: _____

BUSINESS ASSOCIATE - LifeMed ID, Inc.

Sig: _____

Name: _____

Title: _____

Date: , 2016





References

Internal

1. Privacy Policy #5, Minimum Necessary: Uses, Disclosures and Requests
2. Privacy Policy #7, Requests for Restrictions of Uses and Disclosures
3. Privacy Policy #8, Requests for Confidential Communications
4. Privacy Policy #11, Accounting of Disclosures

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>