

**Software License and Services Agreement Exhibit:
Business Associate Agreement**

This Business Associate Agreement (“Agreement”) is made by and between the Customer identified on the first page of the Software License and Services Agreement (“Customer”) and InterOperability Bidco, Inc. d.b.a. Rhapsody (“Business Associate”) (collectively, the “Parties”), and modifies any other prior agreement or contract for this purpose.

The effective date (the “Effective Date”) of this BAA is the effective date of the Engagement Letter and/or contracts entered into between Customer and Subcontractor (“Underlying Agreement(s”).

RECITALS

If Rhapsody is a “Covered Entity” or a “Business Associate” and includes “Protected Health Information” (as those terms are defined in 45 CFR § 160.103), the terms of this Business Associate Agreement (“BAA”), hereby apply. The purpose of this Agreement is to comply with the requirements of (i) the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), (ii) the Health Information Technology for Economic and Clinical Health Act of 2009 (“HITECH”), Pub. L. No. 111-5, Title XIII, and (iii) their implementing regulations, including but not limited to 45 C.F.R. parts 142 and 160-164, as may be amended, including the Privacy Rule and the Security Rule (together, the “Rules”).

The Parties acknowledge that new HIPAA rules were published on January 25, 2013, that became effective on March 26, 2013 (the “New Rules”). Covered entities, business associates, and business associates’ subcontractors are to comply with the New Rules in effect as of September 23, 2013.

WHEREAS, Customer and Business Associate have entered into a relationship under which Business Associate may receive, use, obtain, access or create Protected Health Information (“PHI”) from or on behalf of Customer (the “Services”). As provided in the HIPAA Rules, PHI shall include, when applicable, Electronic Protected Health Information (“E PHI”). Business Associate acknowledges having direct compliance obligations under the HIPAA Rules, and is bound to comply with all requirements of the HIPAA Rules made applicable to business associates pursuant to HITECH; and

WHEREAS, HIPAA, Public Law 104-191 and the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. part 160 and part 164, subparts A and E, as amended, require Customer to enter into a contract with Business Associate containing specific requirements pertaining to Business Associate’s use and disclosure of PHI received from, or created or received on behalf of, Customer.

NOW, THEREFORE, for and in consideration of the recitals above and mutual covenants and conditions below, Customer and Business Associate enter into this Agreement, and agree as follows:

1. **DEFINITIONS.** Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in 45 C.F.R. §§ 160.103 and 164.501.
 - a. **“Breach”** means the acquisition, access, use or disclosure of PHI in a manner not permitted under the Privacy Rule, and which has been compromised, as defined in the omnibus rule regarding HIPAA issued by the Office for Civil Rights of the U.S. Department of Health and Human Services (the “Omnibus Rule”). Breach does not include: (i) any unintentional acquisition, access, or use of PHI by a workforce member or individual acting under the authority of Business Associate if such acquisition, access, or use was made in good faith and within the scope of authority of such employee or individual and does not result in further use or disclosure in a manner not permitted under the Privacy Rule; (ii) any inadvertent disclosure by a person who is authorized to access PHI at Business Associate to another person authorized to access PHI at Business Associate, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under the Privacy Rule; or (iii) a disclosure of PHI where Business Associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.
 - b. **“Designated Record Set”** means: (i) medical records, billing records, enrollment, payment, claims adjudication, and case or medical management records systems maintained by or for Customer; or (ii) records used, in whole or in part, by or for Customer, or the covered entities to which Customer provides business associate services, to make decisions about individuals. For purposes of this definition, the term “record” means any item, collection or grouping of information that includes PHI and is maintained, collected, used or disseminated by or for Customer.

- c. **“Electronic Protected Health Information”** means information that comes within paragraphs 1(i) or 1(ii) of the definition of “protected health information,” as defined in 45 C.F.R. § 160.103, limited to the information created, received, maintained or transmitted by Business Associate on behalf of Customer.
- d. **“Individual”** has the same meaning as the term “individual” in 45 C.F.R. § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).
- e. **“HITECH Act”** means Title XIII and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Public Law No. 111-5, and the regulations enacted thereunder.
- f. **“Privacy Rule”** means the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. part 160 and part 164, subparts A and E.
- g. **“Protected Health Information”** or **“PHI”** has the same meaning as the term “protected health information” in 45 C.F.R. § 160.103, limited to the information created or received by Business Associate from or on behalf of Customer.
- h. **“Required By Law”** has the same meaning as the term “required by law” in 45 C.F.R. § 164.103.
- i. **“Secretary”** means the Secretary of the U.S. Department of Health and Human Services or his designee.
- j. **“Security Incident”** has the same meaning as the term “security incident” in 45 C.F.R. § 164.304.
- k. **“Security Rule”** means the Security Standards and Implementation Specifications at 45 C.F.R. part 160 and part 164, subpart C.
- l. **“Unsecured PHI”** means PHI that is not secured through the use of a technology or methodology that the Secretary specifies in guidance renders PHI unusable, unreadable or indecipherable to unauthorized individuals.

2. PERMITTED USES AND DISCLOSURES

- a. Provision of Services. Business Associate may use and disclose PHI solely for the purpose of providing the Services to Customer.
- b. Other Permitted Uses. Business Associate may use PHI, if necessary: (i) for the proper management and administration of the Business Associate; and (ii) to carry out the legal responsibilities of the Business Associate.
- c. Other Permitted Disclosures. Business Associate may disclose PHI, if necessary, for the purposes described in Section 2.b if: (i) the disclosure is Required By Law; or (ii) Business Associate obtains reasonable assurance from the person or entity to whom the information is disclosed that it will remain confidential and will be used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person or entity, and the person or entity notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.
- d. Pursuant to an Authorization. Business Associate may use or disclose PHI pursuant to a valid authorization by an Individual that satisfies the requirements of 45 C.F.R. § 164.508 and strictly for the purposes designated under the Business Associate’s Agreement.

3. OBLIGATIONS OF BUSINESS ASSOCIATE

- a. Prohibition on Unauthorized Use or Disclosure. Business Associate will not use or disclose PHI, except as permitted or required by the Privacy Rule, the Security Rule, this Agreement and the Agreement to which it is attached as an Addendum, or as Required By Law.
- b. Minimum Necessary. Business Associate shall limit its use and disclosure of PHI under this Agreement to the “minimum necessary” as set forth in guidance that the Secretary issues under the Privacy Rule, or if guidance has not been issued, to the Limited Data Set (as defined by HIPAA) or the minimum necessary to carry out Business Associate’s duties.
- c. The Parties agree that Sections 3.a and 3.b do not apply to: (1) disclosures to, or requests by, a health care provider for treatment; (2) uses or disclosures made to the Individual; (3) disclosures made pursuant to an authorization as set forth in 45 C.F.R. § 164.508; (4) disclosures made to the Secretary under 45 C.F.R. part 160, subpart C; (5) uses or disclosures that are Required by Law as described in 45 C.F.R. § 164.512(a); and (6) uses or disclosures that are required for compliance with applicable requirements of the Privacy Rule.

- d. Safeguards. Business Associate will use appropriate safeguards to prevent the use or disclosure of PHI other than as provided for by this Agreement. Business Associate will implement administrative, physical and technical safeguards as required by the Security Rule, and that reasonably and appropriately protect the confidentiality and integrity of the Electronic Protected Health Information that it receives, maintains or transmits on behalf of Customer. To the extent required by a specific Federal entity, the Business Associate must have the capacity to transport, or transmit Customer sensitive information in an encrypted form, using Customer-approved encryption tools that at a minimum, are or equivalent to FIPS 140-2 validated. Business Associate also agrees to encrypt the storage of identifying information, which will be stored separately from clinical information.
- e. Duty to Report Violations. Business Associate agrees to promptly report to Customer any use or disclosure of PHI by Business Associate not provided for by the Privacy Rule, the Security Rule or this Agreement of which it becomes aware. Business Associate agrees to report to Customer any Security Incident of which it becomes aware. If a breach occurs, Business Associate also agrees to cooperate and assist in any steps taken by Customer to mitigate and address the breach.

As soon as reasonably possible and in all cases, within ten (10) business days of the first day on which any employee, officer, or agent of Business Associate either knows or, by exercising reasonable due diligence, would have known that a Breach of Unsecured PHI has occurred, Business Associate shall notify Customer of such Breach. The notification shall include the identification of each Individual whose Unsecured PHI has been, or is reasonably believed by Business Associate to have been, accessed, acquired, used, or disclosed during such Breach. The notification shall also include: (1) a brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known; (2) recommended steps that Individuals should take to protect themselves from potential harm resulting from the Breach; and (3) a brief description of what Business Associate is doing to investigate the Breach, to mitigate harm to Individuals, and to protect against any further Breaches. Business Associate shall maintain evidence to demonstrate that any required notification under this paragraph was made unless Business Associate determines that a delayed notification applies.

- f. Subcontractors and Agents. Business Associate agrees to ensure that any subcontractor or agent permitted under a subcontract, and to whom it provides PHI, in any course or dealing, agrees in writing to substantially the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information. Business Associate will ensure that any agent, including a subcontractor, to whom it provides Electronic Protected Health Information, agrees to implement reasonable and appropriate safeguards to protect it. Personnel Data made available to Business Associate by Customer for the performance or administration of this Agreement shall be used only for those purposes and shall not be used in any other way without the prior written approval of the Customer. This clause expressly limits Business Associate's and its subcontractors' rights to use data as described in Rights in Data – General, FAR 52.227-14(d)(1).
- g. Inspection of Books and Records. Without limiting the operation of any provision of Section 5 below, and at least ten (10) days' written notice, Business Associate agrees to make its internal practices, books, and records relating to the use and disclosure of PHI available to Customer or, at the request of Customer, to the Secretary in a time and manner designated by Customer or the Secretary for purposes of the Secretary determining Customer's compliance with the Privacy Rule.
- h. Security Regulations. The Parties acknowledge that effective on and after February 17, 2010, 45 C.F.R. §§ 164.308 (administrative safeguards), 164.310 (physical safeguards), 164.312 (technical safeguards), and 164.316 (policies and procedures and documentation requirements) apply to Business Associate in the same manner that such sections apply to Customer. In addition, the requirements of the HITECH Act that relate to security and privacy in Title XIII and Subtitle D respectively, apply to business associates.
- i. Report Pattern or Practice of Activity in Breach. If required under Section 13404 of the HITECH Act, if Business Associate knows of a pattern of activity or practice of Business Associate that constitutes a material breach or violation of the Customer's obligation under this Agreement, Business Associate shall take reasonable steps to cure the breach or end the violation, and, if such steps are unsuccessful, terminate the Agreement or report the problem to the Secretary if termination is infeasible.
- j. Applicable Laws and Compliance with Federal Standards. Business Associate is fully responsible and accountable for ensuring compliance with HIPAA and the Privacy Act. All external internet connections to Customer's network involving Customer information must be reviewed and approved by Customer prior to implementation. Business Associate must receive, gather, store, back up, maintain, use, disclose and dispose of Customer information only in compliance with the terms of this Agreement, and applicable Federal confidentiality and security laws, regulations and policies. If Federal confidentiality and security laws, regulations and policies become applicable to

Customer information or information systems after execution of this Agreement, the Parties agree to negotiate in good faith to implement the information confidentiality and security laws, regulations and policies in this Agreement.

4. OBLIGATIONS OF CUSTOMER

- a. Safeguards and Appropriate Use of Protected Health Information. Customer is responsible for implementing appropriate privacy and security safeguards to protect its PHI in compliance with HIPAA. Without limitation, it is Customer's obligation to:
 - i. Not include PHI in: (a) information Customer submits to technical support personnel through a technical support request or to community support forums; and (b) Customer's address book or directory information.
 - ii. Implement privacy and security safeguards in the systems, applications, and software Customer controls, configures, and uploads into the Business Associate's Software.
- b. Notice of Revocation of Authorization. Customer will provide Business Associate with any changes in, or revocation of, permission by an Individual to use or disclose PHI, if such changes affect Business Associate's permitted or required uses and disclosures.
- c. Notice of Restriction. Customer will notify Business Associate of any restriction to the use or disclosure of PHI that Customer has agreed to in accordance with 45 C.F.R. §164.522.
- d. Impermissible Requests. Customer will not request that Business Associate use or disclose PHI in any manner that would not be permissible under the Privacy Rule or Security Rule if done by Customer.
- e. Disclosure of PHI. Customer shall notify Business Associate of the identity of the employees of Customer who perform administrative functions for the Customer and who are authorized to handle PHI. To the extent practicable, Customer shall also notify Business Associate each time PHI is given to Business Associate by Customer.

5. LIMITATION ON OBLIGATIONS

- a. Enforceability of Privacy Requirements. Any requirement imposed on Business Associate in Section 3 of this Agreement shall not apply in the event a court of competent jurisdiction determines, in response to a challenge raised by Plan Sponsor, Customer or Business Associate, that the Privacy Rule or Security Rule provision requiring the inclusion of the requirement in this Agreement is unenforceable, invalid, or otherwise inapplicable to the relationship between Business Associate and Customer or to the action that the Secretary may request of Business Associate or Customer.

6. TERM & TERMINATION

- a. Term. The term of this BAA shall be effective as of the Effective Date, and shall terminate when all PHI is returned to Customer or destroyed, or, if it is infeasible to return or destroy PHI, protections are extended to such PHI, in accordance with the termination provisions of this Section 6.
- b. Termination for Cause. Upon knowledge of a material breach of this Agreement by Business Associate, Customer shall provide written notice of the breach and provide an opportunity for Business Associate to cure the breach or end the violation within thirty (30) days of such written notice, unless cure is not possible. If Business Associate fails to cure the breach or end the violation within the specified time period or cure is not possible, this Agreement shall automatically and immediately terminate, unless termination is infeasible. In the event Customer must act to cure the breach, then any and all costs, damages, losses, or claims related to such cure shall be fully indemnified, without limitation, by Business Associate.
- c. Termination Upon Notice. This Agreement may be terminated by either party at any time by giving notice to the other party at least sixty (60) days, or a shorter time upon written mutual agreement, prior to the termination.
- d. Effect of Termination. Except as provided in paragraph (b) of this Section 6, upon termination of this Agreement, for any reason, Business Associate shall return or destroy PHI in whatever form or medium and retain no copies of such PHI. Business Associate will complete such return or destruction as soon as possible, but in no event later than sixty (60) days from the date of the termination of this Agreement. In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Customer notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties

that return or destruction of PHI is infeasible, Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

7. MISCELLANEOUS

- a. Regulatory References. A reference in this Agreement to a section in the Privacy Rule, the Security Rule or the Omnibus Rule means the section as in effect or as amended, and for which compliance is required.
- b. Amendment. Business Associate and Customer agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Customer to comply with the requirements of the Privacy Rule, the Security Rule and any other laws applicable through this Agreement.
- c. Survival. The respective rights and obligations of Business Associate under Sections 6.4 of this Agreement shall survive the termination of this Agreement.
- d. Interpretation. Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Customer to comply with the Privacy Rule and the Security Rule.
- e. Governing Law. To the extent that this Agreement is not governed by the requirements of HIPAA and other applicable Federal law, the Agreement is governed by the laws of the Commonwealth of Massachusetts, without reference to the Commonwealth's choice of law rules.
- f. Third Party Beneficiaries. Except as stated herein, nothing express or implied is intended to confer or create, nor be interpreted to confer or create, any rights, remedies, obligations or liabilities to or for any third party beneficiary.
- g. Responsible Person.
 - (i) Business Associate. The following person or, if no person is identified, the person holding the following title is authorized to act on behalf of Business Associate, and receive any notice required to be provided by Customer to Business Associate under any provision in this Agreement:

InterOperability Bidco, Inc. d.b.a. Rhapsody
Attn: Legal Department
100 High Street, Suite 1560
Boston, MA 02110
Legal@rhapsody.health (Not valid for notices)
 - (ii) Customer. To the extent notice is required to be provided by Business Associate to Customer under any provision in this Agreement, notice shall be provided to the contact and address listed in the Underlying Agreement.

Entire Agreement. This BAA, along with any Underlying Agreement which incorporates this BAA by reference, constitutes the entire understanding and obligation of the parties with respect to the subject matter hereof and supersedes any prior agreements, writings or understandings, whether oral or written with respect to the subject matter hereof.