

## **HIPAA BUSINESS ASSOCIATE AGREEMENT**

READ CAREFULLY THIS HIPAA BUSINESS ASSOCIATE AGREEMENT (“AGREEMENT”), WHICH CONTAINS THE EXCLUSIVE TERMS AND CONDITIONS BETWEEN ORCHESTRA ONE, INC. (“BUSINESS ASSOCIATE”), AND YOU (TOGETHER WITH THE ENTITY FOR WHICH YOU REGISTER, ACCESS OR USE THE SERVICE, “COVERED ENTITY”), REGARDING THE SHARING OF ANY PHI PURSUANT TO A SERVICES AGREEMENT (AS DEFINED HEREIN). YOU REPRESENT AND WARRANT THAT YOU HAVE FULL LEGAL AUTHORITY TO ENTER INTO THIS AGREEMENT, UNDER ALL APPLICABLE LAWS AND ON BEHALF OF COVERED ENTITY. BY SELECTING THE “ACCEPT” BUTTON BELOW OR BY ACCESSING OR USING THE BUSINESS ASSOCIATE’S SOFTWARE PLATFORM AND RELATED SERVICES (“ACCEPTANCE”), YOU WILL CREATE A LEGALLY ENFORCEABLE CONTRACT WHERE COVERED ENTITY AGREES TO BE BOUND BY ALL TERMS AND CONDITIONS OF THIS AGREEMENT WITHOUT MODIFICATION.

IF YOU CANNOT OR DO NOT AGREE TO ALL TERMS AND CONDITIONS IN THIS AGREEMENT, YOU SHOULD SELECT THE “DO NOT ACCEPT” BUTTON BELOW AND YOU ARE PROHIBITED FROM ACCESSING OR USING THE SERVICE.

WHEREAS, Business Associate and Covered Entity have, or will, enter into a Services Agreement. In connection with Business Associate’s services, Business Associate and Covered Entity anticipate that Business Associate will create or receive Protected Health Information from and/or on behalf of Covered Entity, which information is subject to protection under the Federal Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104191, as amended by the Health Information Technology for Economic and Clinical Health Act, Title XIII of the American Recovery and Reinvestment Act of 2009 (the “HITECH Act”), and related regulations promulgated by the Secretary (“HIPAA”).

WHEREAS, in light of the foregoing and the requirements of HIPAA, Business Associate and Covered Entity agree to be bound by the following terms and conditions.

NOW, THEREFORE, for good and valuable consideration, the receipt and sufficiency of which is hereby acknowledged, the parties agree as follows:

1. **Definitions.**

a. Capitalized terms used, but not otherwise defined, in this BA Agreement shall have the same meaning given to those terms by HIPAA as in effect or as amended from time to time.

b. “Services Agreement” shall mean any present or future agreements, either written or oral, between Covered Entity and Business Associate under which Business Associate provides services to Covered Entity which involve the use or disclosure of Protected Health Information.

## 2. Obligations and Activities of Business Associate.

a. Use and Disclosure. If Protected Health Information is created by or disclosed to Business Associate, Business Associate agrees not to use or disclose Protected Health Information other than as permitted or required by the Services Agreement, this BA Agreement or as Required by Law. Business Associate shall comply with the provisions of this BA Agreement relating to privacy and security of Protected Health Information and all present and future provisions of HIPAA that relate to the privacy and security of Protected Health Information and that are applicable to “business associates,” as that term is defined in HIPAA.

b. Appropriate Safeguards. Business Associate agrees to use appropriate safeguards to prevent the use or disclosure of the Protected Health Information other than as provided for by this BA Agreement. Without limiting the generality of the foregoing sentence, Business Associate will:

i. Implement administrative, organizational, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of Electronic Protected Health Information that it creates, receives, maintains or transmits on behalf of the Covered Entity as required by the Security Rule;

ii. Report to Covered Entity any Security Incident involving Electronic Protected Health Information of which Business Associate becomes aware. Any actual, successful Security Incident will be reported to Covered Entity in writing without unreasonable delay. Any attempted, unsuccessful Security Incident of which Business Associate becomes aware will be reported to Covered Entity orally or in writing on a reasonable basis, as requested by Covered Entity. If HIPAA is amended to remove the requirement to report unsuccessful attempts at unauthorized access, the requirement hereunder to report such unsuccessful attempts will no longer apply as of the effective date of the amendment.

iii. Notify Covered Entity following the discovery of a Breach of Unsecured Protected Health Information in accordance with 45 C.F.R. § 164.410 without unreasonable delay and in no case later than 60 days (or within any shorter deadline imposed by applicable State law) after discovery of the Breach. A Breach is considered “discovered” as of the first day on which the Breach is known, or reasonably should have been known, to Business Associate or any employee, officer or agent of Business Associate, other than the individual committing the Breach. Any notice of a Security Incident or Breach of Unsecured Protected Health Information shall include the identification of each Individual whose Protected Health Information has been, or is reasonably believed by Business Associate to have been, accessed, acquired, or disclosed during such Security Incident or Breach as well as any other relevant information regarding the Security Incident or Breach.

c. Reporting. Business Associate agrees to report, without unreasonable delay, to Covered Entity any use or disclosure of Protected Health Information by Business Associate or a third party to which Business Associate disclosed Protected Health Information not permitted by this BA Agreement of which Business Associate becomes aware.

d. Minimum Necessary Standard. To the extent required by the “minimum necessary” requirements of HIPAA, Business Associate shall only request, use and disclose the minimum amount of Protected Health Information necessary to accomplish the purpose of the request, use or disclosure.

e. Mitigation. Business Associate agrees to take reasonable steps to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this BA Agreement (including, without limitation, any Security Incident or Breach of Unsecured Protected Health Information). Business Associate agrees to reasonably cooperate and coordinate with Covered Entity in the investigation of any violation of the requirements of this BA Agreement and/or any Security Incident or Breach. Business Associate shall also reasonably cooperate and coordinate with Covered Entity in the preparation of any reports or notices required to be made under HIPAA or any other Federal or State laws, rules or regulations, to any Individual (entitled to notice in connection with a Breach), regulatory body, or any third party, provided that any such reports or notices shall be subject to the prior written approval of Covered Entity.

f. Subcontractors. Business Associate shall enter into a written agreement meeting the requirements of 45 C.F.R. §§ 164.504(e) and 164.314(a)(2) with each Subcontractor (including, without limitation, a Subcontractor that is an agent under applicable law) that creates, receives, maintains or transmits Protected Health Information on behalf of Business Associate. Business Associate shall ensure that the written agreement with each Subcontractor obligates the Subcontractor to comply with restrictions and conditions that are at least as restrictive as the restrictions and conditions that apply to Business Associate through this BA Agreement.

g. Access to Designated Record Sets. To the extent that Business Associate maintains Protected Health Information in a Designated Record Set, Business Associate agrees to provide access, at the request of Covered Entity, and in the time and manner designated by the Covered Entity, to Protected Health Information in a Designated Record Set created or received by Business Associate solely on behalf of Covered Entity only, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under HIPAA Regulations. If an Individual makes a request for access to Protected Health Information directly to Business Associate, Business Associate shall notify Covered Entity of the request within ten (10) business days of such request. Covered Entity shall have the sole responsibility to make decisions regarding whether to approve a request for access to Protected Health Information.

h. Amendments to Designated Record Sets. To the extent that Business Associate maintains Protected Health Information in a Designated Record Set, within thirty (30) days of a receipt of a request from Covered Entity for the amendment of an Individual’s Protected Health Information contained in such Designated Record Set, Business Associate agrees to provide such Protected Health Information to Covered Entity for amendment and to incorporate any such amendment(s) to Protected Health Information in the Designated Record Set maintained by the Business Associate pursuant to HIPAA Regulations and in the time and manner designated by the Covered Entity. If an Individual makes a request for an amendment to Protected Health Information directly to Business Associate, Business Associate shall notify Covered Entity of the

request within ten (10) business days of such request. Covered Entity will have the sole responsibility to make decisions regarding whether to approve a request for amendment to Protected Health Information.

i. Access to Books and Records. Business Associate agrees to make its internal practices, books, and records relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Covered Entity available to the Secretary for purposes of the Secretary determining Covered Entity's and Business Associate's compliance with the Privacy Rule.

j. Accountings. Business Associate agrees to, within thirty (30) days of request for an accounting of disclosures of Protected Health Information from Covered Entity, make available to Covered Entity such information as is in Business Associate's possession and as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with HIPAA. If Business Associate receives a request for an accounting directly from an Individual, Business Associate shall forward such request to Covered Entity within ten (10) business days. Covered Entity shall have the sole responsibility to provide an accounting of disclosures.

### 3. Permitted Uses and Disclosures by Business Associate.

a. Services Agreement. Except as otherwise limited in this BA Agreement, Business Associate may use or disclose Protected Health Information to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Services Agreement, provided that such use or disclosure would not violate HIPAA if done by Covered Entity or the minimum necessary policies and procedures of the Covered Entity.

b. Use for Administration of Business Associate. Except as otherwise limited in this BA Agreement, Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate. Covered Entity acknowledges and agrees that proper management and administration of Business Associate includes, without limitation, modifications or upgrades to its software or services, and development of new features or functionality thereof, or new related product or services.

c. Disclosure for Administration of Business Associate. Except as otherwise limited in this BA Agreement, Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that (i) disclosures are Required by Law, or (ii) Business Associate obtains reasonable assurances from the third party to whom the information is disclosed that the third party will (a) protect the confidentiality of the Protected Health Information, and (b) use or further disclose the Protected Health Information only as Required by Law or for the purpose for which it was disclosed to the third party.

d. Data Aggregation. Business Associate may use Protected Health Information to provide Data Aggregation services relating to the Health Care Operations of Covered Entity if required or permitted under this Agreement or the Service Agreement.

e. De-Identified Information. Business Associate may use Protected Health Information to create de-identified health information in accordance with the HIPAA de-identification requirements. Business Associate may disclose de-identified health information for any purpose permitted by law.

#### 4. Obligations of the Covered Entity.

a. Permissible Requests by Covered Entity. Except as set forth in Section 3 of this BA Agreement, Covered Entity shall not request Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the Privacy Rule if done by Covered Entity.

b. Minimum Necessary PHI. When Covered Entity discloses Protected Health Information to Business Associate, Covered Entity shall provide the minimum amount of Protected Health Information necessary for the accomplishment of Business Associate's purpose.

c. Permissions; Restrictions. Covered Entity warrants that it has obtained and will obtain any consents, authorizations and/or other legal permissions required under HIPAA and other applicable law for the disclosure of Protected Health Information to Business Associate. 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. Covered Entity shall not agree to any restriction on the use or disclosure of Protected Health Information under 45 C.F.R. § 164.522 that restricts Business Associate's use or disclosure of Protected Health Information under this BA Agreement unless Business Associate grants its written consent.

d. Notice of Privacy Practices. Except as required under HIPAA or other applicable law, with Business Associate's consent or as set forth in the Services Agreement, Covered Entity shall not include any limitation in the Covered Entity's notice of privacy practices that limits Business Associate's use or disclosure of Protected Health Information under this BA Agreement.

#### 5. Term and Termination.

a. Term. This BA Agreement shall be effective as of the date of this BA Agreement and shall terminate when all of the Protected Health Information provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this Section.

b. Termination Upon Breach. Any other provision of this BA Agreement notwithstanding, either party (the “**Non-Breaching Party**”), upon knowledge of a material breach by the other party (the “**Breaching Party**”), shall provide an opportunity for the Breaching Party to cure the breach or end the violation. If Breaching Party does not cure the breach or end the violation within thirty (30) calendar days, the Non-Breaching Party may terminate: (A) this BA Agreement; and (B) all of the provisions of the Services Agreement that involve the use or disclosure of Protected Health Information. In the event that termination of this BA Agreement is not feasible, in the Non-Breaching Party’s sole discretion, the Non-Breaching Party has the right to report the breach to the Secretary.

c. Effect of Termination.

i. Except as provided in Section 5(c)(ii), upon termination of this BA Agreement, for any reason, Business Associate shall return or destroy all Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to Protected Health Information that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the Protected Health Information.

ii. In the event that Business Associate reasonably determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall extend the protections of this BA Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such Protected Health Information. Covered Entity acknowledges and agrees that (i) it is infeasible for Business Associate to delete Practice Protected Health Information from its backup tapes or other backup systems and (ii) it is infeasible for Business Associate to delete all Practice Protected Health Information during an ongoing investigation in connection with a Security Incident or Breach of Unsecured Protected Health Information, and that temporarily retaining certain Practice Protected Health Information may be necessary for such investigation.

6. Compliance with HIPAA Transaction Standards. When providing its services and/or products, Business Associate shall comply with all applicable HIPAA standards and requirements (including, without limitation, those specified in 45 CFR Part 162) with respect to the transmission of health information in electronic form in connection with any transaction for which the Secretary has adopted a standard under HIPAA (“Covered Transactions”). Business Associate will make its services and/or products compliant with HIPAA’s standards and requirements no less than thirty (30) days prior to the applicable compliance dates under HIPAA. Business Associate represents and warrants that it is aware of all current HIPAA standards and requirements regarding Covered Transactions, and Business Associate shall comply with any modifications to HIPAA standards and requirements which become effective from time to time. Business Associate shall require all of its agents and subcontractors (if any) who assist Business Associate in providing its services and/or products to comply with the terms of this Section 6.

7. Miscellaneous.

a. Regulatory References. A reference in this BA Agreement to a section in HIPAA, means the section as in effect or as amended or modified from time to time, including any corresponding provisions of subsequent superseding laws or regulations.

b. Amendment. The Parties agree to take such action as is necessary to amend the Services Agreement from time to time as is necessary for the parties to comply with the requirements of HIPAA.

c. Survival. The respective rights and obligations of Business Associate under Section 5(c) of this BA Agreement shall survive the termination of the Services Agreement or this BA Agreement.

d. Interpretation. Any ambiguity in this Agreement shall be resolved to permit the parties to comply with HIPAA.

e. Miscellaneous. The terms of this BA Agreement are hereby incorporated into the Services Agreement. To the extent that Business Associate receives Protected Health Information from or on behalf of Covered Entity and except as otherwise set forth in Section 7(d) of this BA Agreement, in the event of a conflict between the terms of this BA Agreement and the terms of the Services Agreement, the terms of this BA Agreement shall prevail. The terms of the Services Agreement which are not modified by this BA Agreement shall remain in full force and effect in accordance with the terms thereof. This BA Agreement shall be governed by, and construed in accordance with, the laws of the State of California, exclusive of conflict of law rules. Each party to this BA Agreement hereby agrees and consents that any legal action or proceeding with respect to this BA Agreement shall only be brought in the courts of the state where the Covered Entity is located in the county where the Covered Entity is located. The Services Agreement together with this BA Agreement constitutes the entire agreement between the parties with respect to the subject matter contained herein, and this BA Agreement supersedes and replaces any former business associate agreement or addendum entered into by the parties. This BA Agreement may be executed in counterparts, each of which when taken together shall constitute one original. Any PDF or facsimile signatures to this BA Agreement shall be deemed original signatures to this BA Agreement. No amendments or modifications to the BA Agreement shall be effected unless executed by both parties in writing.