Business Associate Agreement

Pursuant to and in compliance with the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), and the regulations promulgated there under, the HIPAA Privacy Regulations, including, but not limited to, 45 C.F.R. Parts 160 and 164, Subpart A and Subpart E (hereinafter the "Privacy Rule"), and HIPAA Security Regulations, including but not limited to, 45 C.F.R. Parts 160 and 164, Subpart A and Subpart C (hereinafter the "Security Rule"), the Health Information Technology for Economic and Clinical Health Act, as incorporated in the American Recovery and Reinvestment Act of 2009 (the "HITECH Act"), and its implementing regulations and guidance issued by the Secretary of the Department of Health and Human Services (the "Secretary"), and all other applicable state and federal laws, as all amended from time to time, including as amended by the Final Rule of 2013, titled "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under the HITECH and the Genetic Information Non-Discrimination Act ("GINA") ("Omnibus Rule"), all business associates of entities such as Customer must agree in writing to certain mandatory provisions regarding the use and disclosure of certain Individually Identifiable Health Information.

Sansio and Customer agree that this Agreement replaces in its entirety any previous Business Associate Agreement between the parties and/or Section 12 of any Subscription Agreement executed on or before September 23, 2013. In order to satisfy the above applicable requirements, the Parties agree as follows effective as of the Compliance Date(s):

A. Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in the Privacy Rule, Security Rule, the HITECH Act, and the Omnibus Rule:

a. Administrative Safeguards. "Administrative Safeguards" shall mean administrative actions, policies, and procedures to manage the selection, development, implementation, and maintenance of security measures to protect Electronic PHI and to manage the conduct of the workforce in relation to the protection of that information.

b. Breach. "Breach" shall mean the unauthorized acquisition, access, use, or disclosure of unsecured PHI which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to obtain such information.

c. Business Associate. "Business Associate" shall mean Sansio.

d. Covered Entity. "Covered Entity" shall mean the Customer.

e. Designated Record Set. "Designated Record Set" shall mean a group of records maintained by or for Sansio or Customer that is: (i) the medical records and billing records about individuals maintained by Sansio or Customer; (ii) the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or (iii) used, in whole or in part, by or for Customer to make decisions about individuals. As used herein, the term "Record"

means any item, collection, or grouping of information that includes PHI and is created, received, maintained, or transmitted by or for Sansio or Customer.

f. Electronic Health Record. "Electronic Health Record" shall mean an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff.

g. Electronic Protected Health Information. "Electronic Protected Health Information" shall have the same meaning as the term "electronic protected health information" in 45 C.F.R. § 160.103, limited to the information that Business Associate creates, receives, maintains, or transmits on behalf of Covered Entity.

h. HIPAA. "HIPAA" shall mean the Health Insurance Portability and Accountability Act of 1996, and any amendments thereto.

i. HITECH. "HITECH" shall mean the Health Information Technology for Economic and Clinical Health Act, which is Title XIII of the American Recovery and Reinvestment Act of 2009, and any amendments, regulations, rules, and guidance issued thereto and the relevant dates for compliance, including amendments to HIPAA as applicable.

j. Individual. "Individual" shall have the same meaning as the term "individual" in 45 CFR § 164.501 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

k. Individually Identifiable Health Information. "Individually Identifiable Health Information" shall mean information that is a subset of health information, including demographic information collected from an individual, and

(i) is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse; and

(ii) relates to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; and (i) identifies the individual, or (ii) with respect to which there is a reasonable basis to believe the information can be used to identify the individual.

l. Omnibus Rule. "Omnibus Rule" shall mean the Final Rule of 2013, titled "Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules under HITECH and the Genetic Information Non-discrimination Act ("GINA").

m. "Physical Safeguards" shall mean physical measures, policies, and procedures to protect electronic information systems and related facilities and equipment from natural and environmental hazards and unauthorized intrusion.

n. Privacy Rule. "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.

o. Protected Health Information. "Protected Health Information" or "PHI" shall mean Individually Identifiable Health Information that is (i) transmitted by electronic

media; (ii) maintained in any medium constituting electronic media; or (iii) transmitted or maintained in any other form or medium. "PHI" shall not include education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. § 1232g, or records described in 20 U.S.C. § 1232g(a)(4)(B)(iv). "PHI" shall have the same meaning as the term "protected health information" in 45 CFR § 164.501, limited to the information created or received by Sansio from or on behalf of Customer.

p. Required By Law. "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR § 164.501.

q. Secretary. "Secretary" shall mean the Secretary of the United States Department of Health and Human Services or his/her designee.

r. Security Incident. "Security Incident" shall mean the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

s. Security Rule. "Security Rule" shall mean the Standards for Security of Individually Identifiable Health Information at 45 CFR parts 160 and 164, subparts A and C.

t. Technical Safeguards. "Technical Safeguards" shall mean the technology, and the policy and procedures for its use that protects Electronic PHI and controls access to it.

u. Transaction Standards. "Transaction Standards" shall mean the Standards for Electronic Transactions, 45 C.F.R. 160 and 162.

v. Unsecured PHI. "Unsecured PHI" shall mean PHI not secured through the use of a technology or methodology specified in guidance by the Secretary that renders PHI unusable, unreadable, or indecipherable to unauthorized individuals.

B. Compliance with Applicable Law. Sansio acknowledges and agrees that in the course of performance of Sansio's obligations under this Agreement, Sansio might be given or obtain access to information which contains Protected Health Information. Beginning with the relevant effective dates, Sansio shall comply with its obligations under this Agreement and with all obligations of a business associate under HIPAA, HITECH, the Omnibus Rule, and other related laws and any implementing regulations, as they exist at the time this Agreement is executed and as they are amended, for so long as this Agreement is in place.

C. Uses and Disclosures of PHI. Except as otherwise limited in this Business Associate Agreement, Sansio may use and disclose Protected Health Information for, or on behalf of, Customer as specified in the Sansio Subscription Agreement. Sansio will not, and shall ensure that its directors, officers, employees, and agents do not, use or further disclose PHI received from Customer other than as permitted or required by this Agreement or as required by law. All uses and disclosures of and requests by Sansio for PHI are subject to the minimum necessary rule of the Privacy Standards and shall be limited to the information contained in a limited data set, to the extent practical, unless additional information is needed to accomplish the intended purpose, or as

otherwise permitted in accordance with Section 13405(b) of HITECH and any implementing regulations.

Customer will provide Sansio with any changes in, or revocation of, permission by an Individual to use or disclose PHI, if such changes affect Sansio's permitted or required uses or disclosures.

D. Customer Responsibilities. Customer will notify Sansio of any restrictions to the use or disclosure of PHI that Customer has agreed to in accordance with 45 C.F.R. § 164.522, to the extent such restrictions affect Sansio permitted or required uses or disclosures.

Customer shall not request Sansio to use or disclose Protected Health Information in any manner that would not be permissible under HIPAA if done by a Covered Entity (unless permitted by HIPAA for a Business Associate).

Customer is responsible for implementing appropriate privacy and security safeguards to protect its Protected Health Information in compliance with HIPAA. Without limitation, it is Customer's obligation to not include Protected Health Information in non-secure channels such as email or information Customer submits to Sansio technical support personnel through a technical support request.

E. Required Safeguards To Protect PHI. Sansio will use appropriate safeguards to prevent use or disclosure of PHI other than as provided for by this Agreement. Sansio agrees to use appropriate administrative, physical, and technical safeguards to protect the confidentiality, integrity, and availability of any electronic PHI in accordance with the Privacy Rule, the Security Rule, and in accordance with Section 13401(a) of HITECH and any implementing Regulations.

Sansio will maintain liability coverage indemnifying Sansio against losses or damages arising out of its treatment of PHI in performing this Agreement, with per occurrence limits not less than $2,000,000.

F. Ownership of PHI. Under no circumstances shall Sansio be deemed in any respect to be the owner of any PHI used or disclosed by or to Sansio pursuant to the terms of the Agreement. Sansio acknowledges that all rights, title, and interest in and to any PHI furnished to Sansio rests solely and exclusively with the Customer or the Individual to whom such PHI relates.

G. Reporting of Improper Use and Disclosures of PHI. Sansio will report to Customer, as soon as reasonably practical, any use or disclosure of PHI not provided for by this Agreement of which Sansio becomes aware.

H. Reporting of Breaches of Unsecured PHI. Sansio shall report to Customer, as soon as reasonably practical, a breach of Unsecured PHI, of which it reasonably becomes aware, in accordance with Section 13402(b) of HITECH.

I. Agreements by Third Parties. Sansio will ensure that any agent, including a subcontractor, to whom Sansio provides electronic PHI created by, received from, maintained for or transmitted by Sansio on behalf of Customer agrees to the same business associate restrictions, terms, conditions, and requirements that apply to Sansio with respect to such information, including without limitation compliance with Section D hereof.

J. Access to Protected Health Information. Sansio will, at the request of Customer, make available PHI maintained by Sansio in a Designated Record Set to Customer in order for Customer to meet the requirements under 45 C.F.R. § 164.524. In the event any Individual delivers directly to Sansio a request for access to PHI, Sansio will forward such request to Customer in order for Customer to respond to such Individual.

K. Availability of PHI for Amendment. Sansio will, at the request of Customer, make available for amendment, and allow Customer to incorporate any amendment(s) in, any Protected Health Information in a Designated Record Set maintained by Sansio, which the Customer directs or agrees to pursuant to 45 C.F.R. § 164.526. In the event any Individual delivers directly to Sansio a request to amend PHI, Sansio will forward such request to Customer, in order for Customer to respond to such Individual.

L. Documentation of Disclosures. Sansio agrees to document disclosures of PHI and information related to such disclosures as would be required for Customer to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528. At a minimum, Sansio shall provide Customer with the following information: (i) the date of the disclosure; (ii) the name of the entity or person who received the PHI, and if known, the address of such entity or person; (iii) a brief description of the PHI disclosed; and (iv) a brief statement of the purpose of such disclosure which includes an explanation of the basis for such disclosure.

M. Accounting of Disclosures. Within ten (10) days of notice by Customer to Sansio that it has received a request for an accounting of disclosures of PHI regarding an Individual during the six (6) years prior to the date on which the accounting was requested, Sansio shall make available to Customer information collected in accordance with Section K of this Agreement, to permit Customer to respond to the request for an accounting of disclosures of PHI, as required by 45 C.F.R. § 164.528. In the case of an Electronic Health Record maintained or hosted by Sansio on behalf of Customer, the accounting period shall be three (3) years and the accounting shall include disclosures for treatment, payment, and healthcare operations, in accordance with the applicable effective date of Section 13402(a) of HITECH. In the event an Individual directly requests an accounting of disclosures, Sansio shall forward such request to Customer in order for Customer to respond to such Individual. Sansio hereby agrees to implement an appropriate record keeping process to enable it to comply with the requirements of this Section.

N. Compliance with HIPAA Transaction Standards. Customer and Sansio each agree to comply with all applicable HIPAA standards and requirements, (including without

limitation, those specified in C.F.R. § 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").

O. Availability of Books and Records. Sansio agrees to make Sansio's internal practices, books, and records relating to the use and disclosure of PHI received from, or created or received by Sansio on behalf of, Customer available to the Secretary for purposes of determining Customer's compliance with the Privacy Rule, Security Rule and the HITECH Act.

P. Effect of Termination of Agreement. Upon termination of this Agreement for any reason, if feasible, Sansio will return or destroy all Protected Health Information created by, received from or maintained by Sansio on behalf of Customer. In the event that Sansio determines that returning or destroying the Protected Health Information is infeasible, Sansio will extend the protections of this 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 Sansio maintains such Protected Health Information.

Q. Red Flag Rules. So long as Sansio retains any confidential or non-public Individually Identifiable Information, Sansio will develop, maintain, and implement policies and procedures designed to ensure the privacy, confidentiality, and security of such information, and to prevent, detect, and mitigate against the reasonably foreseeable risks of personal and medical identity theft in compliance with the requirements of law, including, without limitation, the Identity Theft, Red Flags and Address Discrepancies under the Fair and Accurate Credit Transaction Act of 2003 ("Red Flag Rules"). Sansio will cooperate with Customer in evaluating, investigating, and responding to Red Flags or any possible data breach or Identity Theft activity. Notwithstanding anything to the contrary in this Agreement or any other document, this provision shall survive the expiration or sooner termination of this Agreement, and shall inure to the benefit of Customer and its affiliates and agents.

R. Changes in the Law. Sansio may amend this Agreement as appropriate, to conform to any new or revised legislation, rules and regulations to which Sansio is subject now or in the future including, without limitation, HIPAA, HITECH, the Privacy Standards, Security Standards, or Transaction Standards.