

COMMONWELL HEALTH ALLIANCE MEMBER SERVICES AGREEMENT

This COMMONWELL HEALTH ALLIANCE MEMBER SERVICES AGREEMENT (“Agreement”) is made effective as of the date signed by the Alliance (the “Effective Date”), by and between CommonWell Health Alliance Inc. (“Alliance”), and the Alliance member executing this Agreement (“Member”) (collectively the “Parties”).

BACKGROUND

The Alliance has been established to define and promote a national infrastructure with common standards and policies with regard to enabling: (i) HIT suppliers to quickly and accurately identify patients as they transition through care facilities; (ii) providers to locate and access their patients’ records, regardless of where the encounter occurred; (iii) the delivery of a patient-authorized means to simplify management of data sharing consents and authorizations; and (iv) the provision of authentication and auditing services that facilitate trusted data sharing among member systems. In order to further the foregoing mission, Alliance has procured certain services referred to as the Core Commercial Services through its Service Provider pursuant to a Commercial Services Agreement between Alliance and Service Provider (“CSA”), pursuant to which the Alliance is authorized and hereby agrees to resell the Core Commercial Services to Member under the terms and conditions of this Agreement.

For and in consideration of the mutual covenants herein contained, the Parties hereto agree as follows:

SECTION 1: DEFINITIONS

1.1 Defined Terms. Capitalized terms in this Agreement have the meanings set forth herein and on Exhibit A-1.

SECTION 2: CORE COMMERCIAL SERVICES

2.1 Core Commercial Services. During the Term and subject to the terms and conditions of this Agreement, Alliance hereby authorizes Member to: (i) if applicable, embed Service Provider’s APIs in the Member Solution to enable access to the Core Commercial Services; (ii) access and use the Core Commercial Services and the Documentation for the purpose of providing the Core Commercial Services to Customers; and (iii) market, distribute and sublicense the right to access and use the Core Commercial Services to such Customers. Member will be responsible for implementing the applicable Member Interface with the applicable Member Solution for each Customer in a manner that will interoperate with the Core Commercial Services. Member will (a) utilize the Core Commercial Services in accordance with this Agreement and any applicable Documentation and (b) require that Customers may only use the Core Commercial Services at the locations identified in writing to the Alliance.

2.2 Use Restrictions. Member shall, and Member shall require its Customers to, access or use all or any part of the Core Commercial Services only for the purposes specifically set forth in this Agreement, and only in accordance with a compliant implementation of the Alliance Specification, and approved use cases therein. Without limiting the generality of the foregoing, Member otherwise shall not, and Member shall require its Customers to not, do any of the following: (a) market, sell or distribute the Core Commercial Services except as expressly authorized under this Agreement; (b) license or sub-license the Core Commercial Services to any person or entity other than a Customer; (c) make the Core Commercial Services available to any entity other than a Customer; (d) rent, lease, grant a security interest in or otherwise transfer or attempt to transfer any rights in or to the Core Commercial Services; or (e) remove, alter or deface any legends, restrictions, product identification, copyright, trademark or other proprietary notices from the Core Commercial Services.

2.3 Customer Management. Member agrees to institute a Customer management process including

but not limited to: (a) a process to designate and terminate Customers and Users, including the issuance of usernames and passwords, (b) registration of Users, (c) Member and Customer obligations to ensure each User is appropriately credentialed, (d) reporting requirements regarding adverse changes to licensing status, and (e) a process for Member and its Customers to report any adverse changes to User qualifications.

2.4 Service Level Commitment. Alliance will provide the Core Commercial Services in accordance with the service level commitments set forth in Exhibit C-1. Alliance's ability to meet the service levels is dependent on the Member Solution and Member Interface properly functioning with the Core Commercial Services pursuant to the Alliance Specification.

2.5 Modification; Discontinuance; Suspension; Termination. Alliance reserves the right to modify, discontinue, suspend or terminate provisions of the Core Commercial Services, in whole or in part, upon written notification if (a) Alliance determines in its reasonable discretion that such suspension is necessary to comply with any Applicable Law, or (b) immediately if Alliance determines in its reasonable business judgment that the performance, integrity or security of the Core Commercial Services are being adversely impacted or in danger of being compromised, as a result of Alliance's, Member's, Authorized Member's or Customer's access. Alliance will provide written notice of any suspension as soon as reasonably practical given the circumstances.

2.6 Regulatory. Alliance is not responsible for Member or any Customer's (or their respective Users') compliance with any legal or regulatory requirements imposed on or through the use of the Core Commercial Services. Future regulations or industry practices may affect performance of the Core Commercial Services and require Alliance, Service Provider, Member, Customers, Users, or all, to meet additional regulatory requirements or to discontinue using some or all of the Core Commercial Services. In the event a Party receives written notice from a regulatory authority with jurisdiction over such Party, or with jurisdiction over the subject matter of the Core Commercial Services, that orders or advises such Party to alter or discontinue its provision or use of the Core Commercial Services, the Parties will negotiate in good faith to execute an amendment to this Agreement within ninety (90) days after receipt of such notice (or sooner if required by the regulatory authority), in as narrow a manner and scope as is necessary to comply with such notice. If, after the Parties have engaged in good faith negotiations, either Party determines in good faith that such an amendment is not reasonably possible, then such Party may terminate this Agreement upon thirty (30) days' advance written notice.

2.7 Implementation Plan. The Project Coordinators as defined below will create and will follow the implementation plan that specifies the performance of Implementation Services as well as all prerequisite tasks that a Member and Customer shall complete in preparation for, and during, the implementation process ("Implementation Plan") as set forth in Exhibit D. The Implementation Plan may also include hardware, software, environmental, connectivity, and other specifications regarding items or conditions that must be present in Customer's facilities prior to implementation, as well as during Customer's use, of the Core Commercial Services. Each Party will use commercially reasonable efforts to meet its obligations in any Implementation Plan. The Parties understand and acknowledge that the timeframes specified in Exhibit D represent good faith estimates and are subject to change, depending on any number of variables encountered in the implementation process. For example, Customer EMR upgrades may result in extensions of projected deadlines. No Party is obligated to perform to the extent such performance is adversely affected by the other Party's or a Customer's failure to adhere to the Implementation Plan.

SECTION 3: MEMBER OBLIGATIONS

3.1 Business Practices. Member will not make any representations, warranties or guarantees with respect to the specifications, features or functionality of the Services that are inconsistent with or are in addition to the terms and conditions set forth herein.

3.2 Services. Member will use commercially reasonable efforts to provide and support the Member Solution and the Member Interface to its Customers in a manner that facilitates the successful utilization of the Core Commercial Services by the Customer.

3.3 Training Materials. Member will cooperate with Alliance and Service Provider with any Alliance requested efforts to develop training materials for Customers regarding obtaining and documenting consent and consent functionality, as appropriate, for the Core Commercial Services.

3.4 Member Warranties.

3.4.1 General. Member represents that it is duly organized, validly existing and in good standing under the laws of the state in which it was organized or incorporated and that it has full power and authority to enter into and consummate the transactions contemplated in this Agreement. Member further warrants that the execution and performance of this Agreement does not violate the terms of any security agreement, license, or any other contract or written instrument to which it is a party.

3.4.2 Functionality. Member represents that it will provide the Member Interface and Member Solution in all material respects in accordance with the Documentation and in compliance with the Implementation Plan and Alliance Specification. In the event of breach of this warranty, Member will use reasonable efforts to repair or replace the nonconforming portion of Member Interface and Member Solution in a timely manner so that it performs in accordance with such warranty. The obligations in the foregoing sentence shall be the sole and exclusive remedy of the Parties under this Section 3.4.2.

3.4.3 Compliance with Laws. Member represents that it will comply with all Applicable Laws, statutes, ordinances and regulations in performing its obligations or exercising its rights under this Agreement.

3.4.4 Compliance with Alliance Policies. Member represents that it will, and shall require its Customers to, agree to and comply with all applicable policies adopted by the Alliance (“Alliance Policies”), including but not limited to the Data, Security, and Privacy Policy attached hereto as Exhibit B, and as available here: <http://www.commonwellalliance.org/data-and-security/>, and which may be updated from time to time in accordance with the Alliance Amendment Policy. [See: www.commonwellalliance.org].

3.4.5 Minimum Terms. Member represents that it will contractually bind its Users to the Alliance Member Services Agreement End User License Agreement (“EULA”) attached hereto as Exhibit A-2, and available here www.commonwellalliance.org, and which may be updated from time to time in accordance with the below Alliance Amendment Policy.

3.4.6 Alliance Amendment Policy. Alliance Policies and the EULA may be amended by Alliance from time to time provided that Alliance first provides notice and an opportunity for Contributor Members to provide feedback on the draft proposed amendment and an opportunity to object in accordance with this Section 3.4.6.

3.4.6.1 Amendment Notice. Alliance will provide notice of any proposed material amendment to Alliance Policies or the EULA (each an “Amendment Notice”) to all Contributor Members at least ninety (90) calendar days prior to the effective date of the amendment.

3.4.6.2 Feedback Period. Alliance will accept feedback on the proposed amendment from Contributor Members for fifteen (15) calendar days from the date of the Amendment Notice (the “Feedback Period”).

3.4.6.3 Final Amendment Text. After the Feedback Period Alliance will publish the final text of the

proposed amendment (“Final Amendment Text”) for at least forty five (45) calendar days.

3.4.6.4 Objection Period. Contributor Members shall have thirty (30) calendar days from the date of the publication of the Final Amendment Text (“Objection Period”) to advise Alliance in writing if Contributor Member objects to or is reasonably unable to comply with the proposed amendment, and the specific reasons for its objection or inability to comply. Alliance and objecting member shall cooperate in good faith to implement a plan for such member to become compliant with the Final Amendment Text within a reasonable period of time, but in no case more than three (3) months from the end of the Objection Period, unless a further extension or exception is approved for such Member by the BOD.

3.4.6.5 Compliance Exception. Notwithstanding anything to the contrary in this Section 3.4.6, if Alliance determines in its sole and exclusive discretion that an amendment is required in order for Alliance or its Members or Service Providers to comply with or remain in compliance with Applicable Law, Alliance shall not be required to provide an Objection Period, but shall be required to provide at a thirty (30) day advance notice of the amendment.

3.4.7 Carequality Services. The Parties agree that in addition to the Alliance Core Commercial Services (the “Services”), Member has the option to make Carequality Services available to its Customers. In the event Member makes Carequality Services available to a Customer, such services may involve access to, use of, and re-disclosure of information that the Alliance obtains by virtue of being a Carequality Implementer (the “Carequality Services”).

3.4.7.1 Member Obligations. Prior to making Carequality Services available to a Customer, Member represents and warrants that it shall: (a) contractually require such Customers to comply with the Carequality Connection Terms; (b) provide written notice to such Customers that the Carequality Connection Terms constitute a binding written agreement between such Customer and Alliance, and; (c) receive adequate authority and consents from such Customers for Customer to participate in the Carequality Services, including but not limited to any applicable exchange Activity related thereto. “Carequality Connection Terms” means the Carequality terms and conditions, as updated from time to time and available from Carequality, available here: [<https://sequoiaproject.org/>]. For the purpose of this Agreement “Carequality Implementer” has the meaning provided in the Carequality Connection Terms.

3.4.7.2 Alliance and Member Joint Obligations. Alliance and Member agree to cooperate with each other regarding the delivery of the Carequality Services; provided that other than the notification obligations as provided in this paragraph, the terms and conditions of the Agreement apply to Member and Alliance with respect to the Carequality Services, which shall be deemed Core Commercial Services for the purpose of the Agreement. Each party shall: (a) notify the other party as soon as possible with regards to events requiring notification in connection with the Carequality Connection Terms, and; (b) facilitate compliance with Carequality Connection Terms notification obligations between Alliance and its Connections.

3.4.7.3 Carequality Services and Fees. Members who elect to make Carequality Services available to their Customers shall be obligated to pay the Carequality Access Fees and Carequality Implementer Fees in accordance with Exhibit A-3.

SECTION 4: ALLIANCE OBLIGATIONS

4.1 Business Practices. Alliance will not make any representations, warranties or guarantees with respect to the specifications, features or functionality of any Member Solution or Member Interface that are inconsistent with or are in addition to the terms and conditions set forth herein.

4.2 Services. Subject to the terms and conditions of this Agreement, Alliance agrees to provide support to Member and Customers as described in Exhibit C-2.

4.3 Alliance Warranties.

4.3.1 General. Alliance represents that it is duly organized, validly existing and in good standing under the laws of the state in which it was organized or incorporated and that it has full power and authority to enter into and consummate the transactions contemplated in this Agreement. Alliance further warrants that the execution and performance of this Agreement does not violate the terms of any security agreement, license, or any other contract or written instrument to which it is a party.

4.3.2 Functionality. Alliance will provide the Core Commercial Services in all material respects in accordance with the Documentation and in compliance with the Alliance Specification. In the event of a breach of this warranty, Alliance will be given a reasonable opportunity to repair or replace the nonconforming portion of Core Commercial Services in a timely manner so that it performs in accordance with such warranty; provided Alliance will be relieved from its obligation to perform to the extent such performance is adversely affected by Member's or Customer's failure to adhere to its performance obligations under this Agreement, including without limitation obligations under Section 3.4.2, and the End User Terms, as applicable.

4.3.3 Compliance with Laws. Alliance agrees to comply with all Applicable Laws in performing its obligations under this Agreement.

4.3.4 Services Warranty. Alliance warrants to the Member that all Services will be performed in a professional manner by trained and skilled personnel.

SECTION 5: DATA; SECURITY; PRIVACY.

5.1 Alliance and Member.

5.1.1 PHI Access. Member acknowledges that the purpose of the Core Commercial Services is to enable Member, its Users, and/or its Customers (including the Customer's Users) to access and use PHI only in accordance with an approved Alliance Specification, and with the appropriate patient authorizations and consents. Member is responsible for obtaining all necessary consents and authorizations for its own (including its Users') use and disclosure of PHI in its Member Solution regardless of whether the PHI was received through the Core Commercial Services or otherwise. The Parties acknowledge that additional use cases may be added that require changes in compliance obligations.

5.1.2 BAAs. Member represents and warrants that it maintains a valid business associate agreement and any other appropriate agreements with each of its Customers that authorizes access, use and disclosure of Data and PHI as necessary for that Customer's participation in the Core Commercial Services and that Member will comply with its business associate agreements with its Customers in connection with the use of the Core Commercial Services. Member acknowledges that Alliance's and Service Provider's use, access, and disclosure of PHI on behalf of Member and/or its Customers to provide the Core Commercial Services as set forth in this Agreement is permitted under Alliance's business associate agreement with Member.

5.2 Core Commercial Services. Member grants Service Provider the right to use data, including but not limited to Data, PHI and de-identified PHI acquired through the Core Commercial Services, solely for Service Provider to provide the Core Commercial Services; provided Service Provider may de-identify PHI and store Data and de-identified PHI for the sole purposes of performance testing, trouble shooting and improving the Core Commercial Services within the scope of the Agreement for the Alliance and Members, Customers, patients or other members of the Alliance, and for no other purpose, and provided that Service Provider shall not modify, transform, conduct analysis on, or otherwise use data, including but not limited to PHI, de-identified PHI, or Data, in any manner except as necessary to provide the Core Commercial Services and as described in this Section 5.2.

5.3 Alliance Access to PHI. For the avoidance of doubt, reference in this Agreement to use, access, and disclosure of PHI by Alliance shall mean the use, access, and disclosure of PHI on behalf of Alliance

by Service Provider; Alliance, as distinct from Service Provider or any Member, will not have access to any PHI or Data in connection with this Agreement.

SECTION 6: PRICING AND PAYMENT

6.1 Fees and Invoicing Terms. Member shall pay Alliance all fees and charges for the implementation and operation of the Core Commercial Services and any related Services, including the annual subscription fees related thereto, in accordance with Exhibit A-3. The Alliance and Service Provider reserve the right to suspend or terminate the Core Commercial Services and this Agreement for late payments in accordance with the terms related thereto. Member acknowledges Service Provider is a third party beneficiary of Member's payment obligations.

6.2 Expenses. Neither Party will be responsible for expenses incurred by the other relating to the subject matter of this Agreement unless such expenses were authorized in writing by an authorized representative of such Party. Any such expenses must be authorized in advance by the Party, reasonably incurred and documented, and in conformance with its own travel reimbursement policy which will be provided upon request.

6.3 Taxes. All amounts payable in connection with this Agreement are exclusive of sales, use, and value-added taxes and withholding taxes. Each Party is responsible for the payment of its own taxes.

SECTION 7: TERM AND TERMINATION

7.1 Term. The term of this Agreement shall commence on the Effective Date and continue for thirty-six (36) months from the date of the Initial Payment (the "Initial Term"). Unless otherwise defined in Exhibit A-3 of this Agreement, "Initial Payment" shall mean Member's initial Annual Subscription Fee payment, which shall be payable: 1) six (6) months from the Effective Date, or; 2) on the date Member implements the Core Commercial Services, which ever occurs first. At the end of the Initial Term, the Agreement will automatically renew for additional subsequent one (1) year periods (each a "Subsequent Renewal Term" and collectively, the "Term") unless either Party provides notice of its intent not to renew the Agreement at least one hundred and twenty (120) days prior to the end of the then current Term.

7.2 Termination for Cause. Either party may terminate the Agreement upon notice if the other: (i) materially breaches the Agreement and fails to remedy, or fails to commence reasonable efforts to remedy, such breach within sixty (60) days after receiving notice of the breach from the terminating Party, (ii) infringes or misappropriates the terminating Party's (including its licensor's) Intellectual Property Rights and fails to remedy, or fails to commence reasonable efforts to remedy, such breach within thirty (30) days after receiving notice of the breach from the terminating Party, (iii) materially breaches this Agreement in a manner that cannot be remedied, or (iv) commences dissolution proceedings or ceases to operate in the ordinary course of business. Upon written notice, either Alliance or Service Provider may terminate this Agreement if Member is no longer a Member of the Alliance or a party to the Alliance Membership Agreement.

7.3 Transition Services. In order to allow for the orderly transition of the Services upon termination or expiration of this Agreement, pursuant to Sections 7.1 or 7.2, if requested in writing Member may continue to receive Services from Service Provider at the same level as prior to the termination or expiration, and on the same terms (the "Transition Services"), from the date of the termination for up to twelve (12) months after the termination or expiration date (the "Transition Period"). Service Provider will not be obligated to provide Transition Services to Member if Member is in breach any material terms of this Agreement, including Member's obligation to pay applicable fees. The Transition Services shall include Data Migration Services. Data Migration Services shall be available on a time and materials basis from Service Provider, in accordance with an agreement mutually agreed upon between Service Provider and Member. "Data Migration Services" shall mean those services and access necessary for the

transitioning party to complete its transition, including without limitation, access to a person's records and applicable document links.

7.4 Obligations upon Termination. Subject to any Transition Services provided for in Section 7.3, upon the expiration or termination of this Agreement:

7.4.1 Member will promptly cease using and destroy or return to Alliance and Service Provider, at either's request, all advertisements and promotional materials that bear such Service Provider or the Alliance's Marks and all Confidential Information of Alliance and Service Provider;

7.4.2 Member will promptly: (i) cease use of the Core Commercial Services; and (ii) certify in writing to Alliance that Member has complied with its obligations under this Section 7.4.2; and

7.4.3 Each Party will, promptly return to the other Party or destroy all copies (including partial copies) of Confidential Information disclosed by the other Party and certify in writing to the other Party that it has complied with its obligations under this Section 7.4.3. Alliance will cause its Service Provider to comply with the obligations in this Section 7.4.3. Member acknowledges its obligations under this Section 7.4.3 apply to Confidential Information of Service Provider.

7.5 Survival of Provisions. The following provisions of this Agreement shall survive termination or expiration of this Agreement and will remain in full force and effect: 1.1 (Definitions), 7.3 (transition Services), 7.4 (Obligations upon Termination), 7.5 (Survival of Provisions), 8 (Confidentiality), 9.6 (Indemnification), 10 (Limitation of Liability), 11 (General Terms).

SECTION 8: CONFIDENTIALITY

8.1 Confidentiality - Use and Disclosure of Confidential Information. Alliance and Member may disclose to the other Confidential Information. Except as expressly permitted by this Agreement, neither Party will: (1) disclose any other Party's Confidential Information except (x) to its employees, contractors, or service providers, who have a need to know and are bound by confidentiality terms no less restrictive than those contained in this Section 8.1, or (y) to the extent required by Applicable Law following prompt notice of such obligation to the other Party; or (2) use any other Party's Confidential Information for any purpose other than performing its obligations under this Agreement or enjoying the rights granted under this Agreement. Each Party will use reasonable care in handling and securing the other Party's Confidential Information by employing reasonable security measures used for its own proprietary information of similar nature. For the purpose of this Section 8, Member shall include Members, and their employees, contractors, and agents who may receive Confidential Information during their involvement with the Alliance, and Members shall obligate such persons to comply with the obligations of confidentiality in this Agreement.

8.2 Period of Confidentiality. The restrictions on use, disclosure and reproduction of Confidential Information set forth in Section 8.1 will, with respect to Confidential Information that constitutes a "trade secret" (as that term is defined under Applicable Law), be perpetual, and will, with respect to other Confidential Information, remain in full force and effect during the Term and for three years following the termination of this Agreement.

SECTION 9: INTELLECTUAL PROPERTY

9.1 Alliance Specification. Ownership of all right, title and interest in and to the Intellectual Property Rights in the Alliance Specification shall be governed by the terms of the Membership Agreement. Licensing of the Alliance Specification shall be governed by the Membership Agreement and other licenses applicable to the use of the Alliance Specification that are approved and made available by the Alliance.

9.2 Member Ownership. As between Alliance and Member, Member will own all right, title and interest in and to the Member Confidential Information, Member Solution, and Member Materials,

including any and all Intellectual Property Rights therein. The Alliance agrees not to take any step to disassemble, decompile, or reverse engineer or otherwise derive a source code equivalent of the software in the Member Confidential Information or to permit any third party to do so; provided, however, nothing in the foregoing shall prevent Alliance from exercising the rights granted in this Agreement in such Confidential Information. Nothing in this Agreement will be deemed to transfer any ownership interest to Alliance or any other party in such Member Confidential Information, Member Solution and Member Materials or Third Party Materials provided by a Member to Alliance. Any Member Solution, Member Materials or Third Party Materials provided by Member to Alliance and any modifications thereto are, and shall remain, the property of Member or a third party, as applicable.

9.3 Service Provider Ownership. As between Alliance, Member and Service Provider, Service Provider will own all right, title and interest in and to Service Provider Materials, Documentation, Service Provider's Confidential Information including any and all Intellectual Property Rights therein, and all Intellectual Property Rights developed or created by Service Provider or its personnel during the course of performing any Services in connection with this Agreement. Member and Alliance acknowledges that the Service Provider Materials contain trade secrets of Service Provider, and Member and Alliance agree not to take any step to disassemble, decompile, or reverse engineer or otherwise derive a source code equivalent of the software in the Service Provider Materials or to permit any third party to do so. Nothing in this Agreement will be deemed to transfer any ownership interest to Member, Alliance or Customers in Service Provider Confidential Information, Service Provider Materials or Third Party Materials provided by Service Provider to Alliance or Member. Any such Service Provider Materials, Service Provider Confidential Information or Third Party Materials and any modifications thereto are and shall remain, the property of Service Provider or the third party, as applicable, and the licenses to use such materials as set forth in this Agreement constitute all of Member's and Alliance's rights in such materials.

9.4 Feedback and General Knowledge. Member may from time to time identify problems, solutions to identified problems, provide suggestions, comments or other feedback related to the Core Commercial Services, Service Provider Materials, including, without limitation, the Core Commercial Services integration with the Member Solution, whether such information was shared prior to, on or after the Effective Date ("Feedback") to Alliance or Service Provider. Member will not provide Feedback that includes Confidential Information of Member or third party. Member grants Alliance and Service Provider a non-exclusive, royalty-free, fully paid, perpetual, non-revocable, sub-licensable, license in and to its Intellectual Property Rights (except for any patent or trademark rights) in and to its Feedback to develop, manufacture, make, have made, reproduce, have reproduced, modify, use, export, import, create derivative works of, offer to sell and sell such Feedback with the Core Commercial Services or other Service Provider products and services or to grant others the right to do so. Each Party retains the right to use any generalized knowledge, ideas, concepts, techniques, methodologies, practices, processes and know-how learned by its personnel in the course of performing services in connection with this Agreement, whether learned prior to, on or after the Effective Date.

9.5 No Implied Rights. Except as may be expressly stated in writing, nothing contained herein or implied pursuant to the business relationship between the Parties shall be construed to give any rights or interests to one Party in the rights or interests of any other Party in such Party's Intellectual Property Rights.

9.6 Intellectual Property Infringement Indemnification by Member.

9.6.1 Duty to Defend and Indemnification. Member will defend, indemnify, and hold the Alliance and the Service Provider ("Indemnified Parties") harmless, from any action or other proceeding brought by a third party against the Indemnified Parties at Member's sole cost and expense to the extent that such action or proceeding is based on a claim by a third party that (a) the use or sale of the Member Materials or Member Solution infringes any U.S. copyright or U.S. patent, (b) the Member Materials or Member Solution incorporate any misappropriated trade secrets, or (c) any Member trademark or service mark provided by Member infringes any U.S. trademark or service mark. Member will pay any damages finally awarded against Indemnified Parties, including any award of costs, as a result thereof; provided, that the Indemnified Parties (i) notifies Member of the claim as promptly as practical, but in any event

timely enough so as not to prejudice any defense, (ii) provides Member with all reasonably requested cooperation, information and assistance, and (iii) gives Member sole authority to engage defense counsel, control the litigation, and defend and settle the claim at the Member's sole cost and expense. For the avoidance of doubt, so long as the Member is satisfying the obligation to the Indemnified Parties to defend and settle the claim at the Member's sole cost and expense, the Member will not be obligated to reimburse Indemnified Parties for any attorneys' fees for attorneys engaged by any Indemnified Party or other costs and expenses incurred at the direction of any Indemnified Party to defend or settle the claim. For the avoidance of any doubt, with respect to any claims that are Member Combination Claims (as defined in Section 9.6.2 below), Member will indemnify the Indemnified Parties for expert witness fees for experts engaged by both Member and the Indemnified Parties, but will not indemnify the Indemnified Parties for expert witness fees or other costs solely attributable to the Indemnified Party, such as e-discovery costs.

9.6.2 Exclusions. Member will have no obligations under Section 9.6.1 to the extent a claim arises from any use by Indemnified Parties of Member Materials, Member Solutions, or Member trademarks in a manner not contemplated by this Agreement or the Documentation, or use of the Member Materials or Member Solutions in combination with products, services or activities not provided by Member unless (i) Member Materials or Member Solutions provided by the Member perform the point(s) of novelty of the invention in the asserted patent, (ii) none of the limitations in any asserted patent claim are met by a design choice made by Indemnified Parties for which there existed a reasonable, non-infringing substitute, and (iii) any limitations of any asserted patent claim(s) that are attributable to products, services or activities of Indemnified Parties combined with the Member Materials or Member Solutions are insubstantial to the point(s) of novelty, for example, the combination of the Member Materials or Member Solutions with a generic network or one or more staple hardware elements (i.e., generic display, storage media) when such combined elements are insubstantial to the point(s) of novelty ("Member Indemnified Combination Claims").

9.6.3 Infringement Remedies. If a claim of infringement or misappropriation for which an Indemnified Party is entitled to be indemnified under Section 9.6.1 arises, then Member may, at its sole option and expense: (a) obtain for an Indemnified Party the right to continue using (i) the Member's trademark, Member Solutions or Member Materials or (ii) terminate the affected Core Commercial Services license and terminate Member's rights and obligations under this Agreement with respect to such Core Commercial Services.

9.6.4 Member as Third-Party Beneficiary. Notwithstanding anything to the contrary in an agreement between Alliance and Service Provider, to the extent Alliance has obtained Warranties and obligations of Indemnification and similar rights from Service Provider related to the delivery of the Core Commercial Services pursuant to this Agreement, Member shall be a third-party beneficiary related to such rights held by the Alliance.

9.6.5 Exclusive Remedy. THE FOREGOING IS MEMBER'S SOLE AND EXCLUSIVE OBLIGATIONS, AND THE INDEMNIFIED PARTIES' SOLE AND EXCLUSIVE REMEDIES, WITH RESPECT TO INTELLECTUAL PROPERTY INFRINGEMENT OR TRADE SECRET MISAPPROPRIATION.

9.7 Trademarks

9.7.1 Limited License to Alliance Marks. Subject to the terms and conditions of this Agreement, Alliance grants Member a non-exclusive, non-transferable right to use and display the Alliance trademarks and service marks provided by Alliance, as may be updated from time to time in Alliance's sole discretion (the "Alliance Marks"), to advertise and promote the Core Commercial Services and otherwise as necessary or appropriate for Member to exercise its rights or perform its obligations under this Agreement, all subject to Member's compliance with the Alliance's Trademark Usage Guidelines, as may be modified from time to time. Member acknowledges and agrees that Alliance owns the Alliance Marks and that any and all goodwill and other proprietary rights that are created by or that result from Member's use of the Alliance Marks inure solely to the benefit of Alliance. Member will not at any time

contest or aid in contesting the validity or ownership of the Alliance Marks or take any action in derogation of Alliance's rights therein, including, without limitation, applying to register any trademark, trade name or other designation that is confusingly similar to any Alliance Mark.

9.7.2 Limited License to Member Marks. Subject to the terms and conditions of this Agreement, Member grants Alliance a non-exclusive, non-transferable right to use and display the Member trademarks and service marks provided by Member, as may be updated from time to time in Member's sole discretion (the "Member Marks"), to advertise and promote the Services and otherwise as necessary or appropriate for Alliance to exercise its rights or perform its obligations under this Agreement. Alliance acknowledges and agrees that Member owns the Member Marks and that any and all goodwill and other proprietary rights that are created by or that result from Alliance's use of the Member Marks inure solely to the benefit of Member. Alliance will not at any time contest or aid in contesting the validity or ownership of the Member Marks or take any action in derogation of Member's rights therein, including, without limitation, applying to register any trademark, trade name or other designation that is confusingly similar to any Member Mark.

SECTION 10: LIMITATION OF LIABILITY

10.1 Total Damages. EXCEPT FOR EACH PARTY'S OBLIGATIONS UNDER SECTION 8 AND MEMBER'S OBLIGATIONS UNDER SECTION 9.6 MEMBER'S TOTAL CUMULATIVE LIABILITY UNDER, IN CONNECTION WITH OR RELATED TO THIS AGREEMENT WILL BE LIMITED TO THE TOTAL FEES PAID AND PAYABLE TO ALLIANCE BY MEMBER IN CONNECTION WITH RECEIVING THE CORE COMMERCIAL SERVICES IN THE EIGHTEEN (18) MONTHS PRIOR TO THE EVENT GIVING RISE TO THE CLAIM, AND THE TOTAL CUMULATIVE LIABILITY OF THE ALLIANCE UNDER, IN CONNECTION WITH OR RELATED TO THIS AGREEMENT WILL BE LIMITED TO TWENTY-FIVE (\$25,000) THOUSAND DOLLARS.

10.2 Exclusion of Damages. EXCEPT FOR EACH PARTY'S OBLIGATIONS UNDER SECTIONS 8 AND MEMBER'S OBLIGATIONS UNDER SECTION 9.6 IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER PARTY, IN CONNECTION WITH, OR RELATED TO THIS AGREEMENT FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, LOST PROFITS OR LOSS OF GOODWILL, WHETHER BASED ON BREACH OF CONTRACT, WARRANTY, TORT, PRODUCT LIABILITY, OR OTHERWISE, AND WHETHER OR NOT ANY PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

10.3 Material Consideration. THE PARTIES ACKNOWLEDGE THAT THE FOREGOING LIMITATIONS ARE A MATERIAL CONDITION FOR THEIR ENTRY INTO THIS AGREEMENT.

10.4 Disclaimer of Warranty. EXCEPT AS SET FORTH IN 3.4.2 and 4.3.2 EACH PARTY PROVIDES ITS CONFIDENTIAL INFORMATION, AND THE ALLIANCE PROVIDES THE CORE COMMERCIAL SERVICES "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. NO PARTY WARRANTS THAT SUCH MEMBER INTERFACE, MEMBER SOLUTION, SERVICE PROVIDER INTERFACE OR THE CORE COMMERCIAL SERVICES WILL MEET ANY OTHER PARTY'S REQUIREMENTS OR THAT THEIR OPERATION WILL BE UNINTERRUPTED OR ERROR FREE. EACH PARTY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

10.5 Data Format, Loss or Damage Disclaimers. ALLIANCE AND MEMBER ACKNOWLEDGE AND AGREE THAT ANY PHI OR DATA, WHETHER IN A RECORD OR OTHERWISE RECEIVED BY ALLIANCE OR SERVICE PROVIDER THROUGH THE CORE COMMERCIAL SERVICES FROM ANY PARTY OR THIRD PARTY, SHALL BE IN A FORMAT THAT CONFORMS WITH SPECIFICATIONS SET FORTH IN THE ALLIANCE SPECIFICATION OR OTHERWISE AGREED UPON BY THE PARTIES IN WRITING. ACCORDINGLY, ALLIANCE DISCLAIMS FOR ITSELF

AND FOR SERVICE PROVIDER ANY AND ALL LIABILITY RESULTING FROM OR RELATED TO INACCURATE DATA OR OMISSIONS OR ERRORS IN THE DATA TRANSMITTED FROM PARTIES OR THIRD PARTIES, INCLUDING INFORMATION SUBMITTED BY PATIENTS OR PROVIDERS THROUGH USE OF THE CORE COMMERCIAL SERVICES. WITHOUT LIMITING THE LIABILITY DISCLAIMERS IN THIS AGREEMENT AND EXCEPT AS OTHERWISE EXPRESSLY PROVIDED IN THIS AGREEMENT, NEITHER ALLIANCE NOR SERVICE PROVIDER IS LIABLE FOR ANY LOSS OF OR DAMAGE TO ANY PHI OR DATA OF MEMBER, ITS USERS OR ITS CUSTOMERS, OR THE UNAVAILABILITY OF ANY OF THE CORE COMMERCIAL SERVICES.

SECTION 11: GENERAL TERMS

11.1 Certification. At Alliance's written request, Member will furnish Alliance with a certification signed by an officer of Member verifying that Member is in compliance with the terms and conditions of this Agreement including with regards to any payment terms or obligations. At Alliance's request, Member will furnish Alliance with any detail or documentation supporting such certification, as reasonably requested by Alliance.

11.2 Export Control. This Agreement is subject to governmental laws, orders and other restrictions regarding the export, import, re-export or use ("Control Laws") of the Core Commercial Services and Documentation, including technical data and related information ("Regulated Materials"). Alliance and Member shall comply, and Member shall cause its Customers and Users to comply, with all Control Laws relating to the Regulated Materials in effect in, or which may be imposed from time to time by, the United States or any country into which any Regulated Materials are shipped, transferred, or released. Alliance and Member may permit use of the Core Commercial Services by any outsourcing or facility management service provider only with Alliance's prior written approval.

11.3 Dispute Resolution and Negotiation.

11.3.1 The Parties shall attempt in good faith to resolve any dispute arising out of or relating to this Agreement ("Dispute") promptly by negotiation between executives who have authority to settle the controversy. A Party may give the other Party written notice of any Dispute not resolved in the normal course of business ("Dispute Notice"). Within fifteen days after delivery of the Dispute Notice, the receiving Party shall submit to the other a written response. The Dispute Notice and response shall include with reasonable particularity (a) a statement of each Party's position and a summary of arguments supporting that position, and (b) the name and title of the executive who will represent that Party and of any other person who will accompany Member's executive. Within thirty (30) days after delivery of the Dispute Notice, the executives of both Parties shall meet at a mutually acceptable time and place. Unless otherwise agreed in writing by the negotiating Parties, the above-described negotiation shall end at the close of the first meeting of executives described above ("First Meeting"). Such closure shall not preclude continuing or later negotiations, if desired.

11.3.2 All offers, promises, conduct and statements, whether oral or written, made in the course of the negotiation by any of the Parties, their agents, employees, experts and attorneys are confidential, privileged and inadmissible for any purpose, including impeachment, in arbitration or other proceeding involving the Parties, provided that evidence that is otherwise admissible or discoverable shall not be rendered inadmissible or non-discoverable as a result of its use in the negotiation. At no time prior to the First Meeting shall either side initiate an arbitration or litigation related to this Agreement except to pursue a provisional remedy that is authorized by Applicable Law or by agreement of the Parties. However, this limitation is inapplicable to a Party if the other Party refuses to comply with the requirements of this subsection. All applicable statutes of limitation and defenses based upon the passage of time shall be tolled while the procedures specified in this subsection above are pending and for fifteen days thereafter. The Parties will take such action, if any, required to effectuate such tolling.

11.3.3 In the event any Dispute is not resolved as set forth above in this Section 11.3, each Party agrees that venue for all actions, relating in any manner to this Agreement, will be in a federal or state court of competent jurisdiction in the state of Delaware. Notwithstanding the foregoing, any Party may apply to any court of competent jurisdiction in the State of Delaware for a temporary restraining order, preliminary injunction, or other interim, conservatory or equitable relief, as necessary, without breach of this Section 11.3 and without any abridgment of the powers of the court. Each Party will maintain the confidentiality of any such Disputes unless such Party reasonably believes such Dispute materially and adversely impacts overall success of the Core Commercial Services by other parties, in such event the Party with such reasonable belief will provide at least ten days written notice to the other Party before notifying any other Member of such Dispute. Member agrees to cooperate with both Alliance and Service Provider following the general guidelines of this Section 11.3 to the extent any dispute involves each of Alliance or Service Provider. Alliance will engage Service Provider to participate in any such dispute at the request of Member.

11.4 Insurance. Member agrees, at its own expense, to maintain policies of commercial general liability insurance, self-insurance, or captive insurance with a minimum limit of \$1,000,000 per occurrence and \$3,000,000 annual aggregate, professional errors and omissions liability insurance with \$1,000,000 per claim and \$3,000,000 annual aggregate, and statutory workers compensation and employers liability coverage with \$1,000,000 limit each accident or disease at its own expense. Member shall, at the written request of Alliance, furnish a certificate of insurance evidencing the maintenance in full force of such insurance.

11.5 Injunctive Relief. The Parties agree that the breach, or threatened breach, of a Party's Confidential Information or Intellectual Property Rights may cause irreparable harm without adequate remedy at law. Upon any such breach or threatened breach, a Party will be entitled to seek injunctive relief to prevent the other Party from commencing or continuing any action constituting such breach, without having to post a bond or other security. Nothing in this Section 11.5 will limit any other remedy available to either Party.

11.6 Books and Records. If required by Section 952 of the Omnibus Reconciliation Act of 1980, 42 U.S.C. Section 1395x(v)(1)(1), for a period of four years after the Services are furnished, each Party agrees to make available, upon the written request of the Secretary of Health and Human Services, the Comptroller General, or their representatives, this Agreement and such books, documents, and records as may be necessary to verify the nature and extent of the Services with a value or cost of \$10,000 or more over a twelve month period.

11.7 Governing Law. This Agreement is governed by and will be construed in accordance with the laws of the State of Delaware, exclusive of its rules governing choice of law and conflict of laws and any version of the Uniform Commercial Code.

11.8 Competition Law Compliance. The Parties agree to conduct their activities in compliance with the spirit and letter of any applicable state and federal competition laws and their existing compliance policies.

11.9 Assignment. Neither Party will assign this Agreement, by operation of law or otherwise, without the prior written consent of the other Party which will not be unreasonably withheld. A change of control constitutes an assignment under this Section 11.9, provided either Party may, upon notice assign this Agreement to any U.S. entities that, in the future, is controlled by or under common control with such Party, as the result of a transfer of all or substantially all of that Party's assets or capital stock or of any other corporate reorganization, provided in each case the Parties remain liable for their obligations under this Agreement.

11.10 Severability. If any part of a provision of this Agreement is found illegal or unenforceable, it will be enforced to the maximum extent permissible, and the legality and enforceability of the remainder of that provision and all other provisions of this Agreement will not be affected.

11.11 Notices. All notices relating to the Parties' legal rights and remedies under this Agreement will be provided in writing and will reference this Agreement. Such notices will be deemed given if sent by: (a) postage prepaid registered or certified U.S. Post mail, then five working days after sending; or (b) commercial courier, then at the time of receipt confirmed by the recipient to the courier on delivery. All notices to a Party will be sent to its address set forth on the signature page of this Agreement, or to such other address as may be designated by that Party by notice to the sending Party.

11.12 Waiver. Failure to exercise or enforce any right under this Agreement will not act as a waiver of such right.

11.13 Force Majeure. Except for the obligation to pay money, a Party will not be liable to the other for any failure or delay caused by a Force Majeure Event, whether or not such matters were foreseeable, and such failure or delay will not constitute a material breach of this Agreement.

11.14 Amendment. This Agreement may be modified, or any rights under it waived, only by a written document executed by the authorized representatives of the Parties.

11.15 Third Party Beneficiaries. Service Provider shall be a third-party beneficiary to the Alliance's rights under Sections: 2.1, 2.2, 2.6, 3, 5.1, 6, 8, 9.3, 9.4, 9.5 and 9.6. Member shall be a third-party beneficiary to any Alliance obtained Warranties and obligations of Indemnification and similar rights Alliance has received from Service Provider in accordance with Section 9.6.4.

11.16 Relationship of Parties. Each Party is an independent contractor of the other Party. This Agreement will not be construed as constituting a relationship of employment, agency, partnership, joint venture or any other form of legal association. Neither Party has any power to bind the other Party or to assume or to create any obligation or responsibility on behalf of the other Party or in the other Party's name.

11.17 Publicity. Neither Party will make any public announcement or press release regarding this Agreement or any activities performed hereunder without the prior written consent of the other Parties.

11.18 Construction of Agreement. This Agreement will not be presumptively construed for or against any Party. Section titles are for convenience only. As used in this Agreement, "will" means "shall," and "include" means "includes without limitation." The Parties may execute this Agreement in one or more counterparts, each of which will be deemed an original and one and the same instrument.

11.19 Entire Agreement. This Agreement, including the Schedules, Exhibits, and documents incorporated by reference, constitute the complete and exclusive agreement between the Parties with respect to the subject matter hereof, superseding and replacing all prior agreements, communications, and understandings (written and oral) regarding its subject matter, including without limitation any letter of intent executed between the Parties. Terms and conditions on or attached to purchase orders will be of no force or effect.

This Agreement is executed by an authorized representative of each Party.

[Signature blocks on next page]



COMMONWELL HEALTH ALLIANCE INC. ALLIANCE MEMBER: _____

Signature: _____

Name: Jitin Asnaani

Title: Executive Director

Date: _____

Signature: _____

Name: _____

Title: _____

Date: _____

Alliance Address:
Jitin Asnaani
75 Arlington Street, Suite 500,
Boston, MA 02116

Attn: Executive Director

Attn: Legal Counsel

Jim Markwith
520 Pike Street
Suite 2500
Seattle, WA 98101

with e-mail to:
jim@markwithlaw.com

Member Name and Contact Information

Full Member Name: _____

Address: _____

Attn: _____

EXHIBIT A-1
MEMBER SERVICES AGREEMENT
DEFINITIONS

“**Agreement**” shall have the meaning set forth in the introductory paragraph of the first page of this agreement.

“**Alliance Specification**” means the current Specification adopted by the Alliance.

“**API**” means application programming interface.

“**Applicable Laws**” means all laws (including common law), statutes, rules, regulations, ordinances, formal written guidance, codes, permits and other authorizations and approvals having the effect of law of the United States, any foreign country or any domestic or foreign state, county, city or other political subdivision.

“**Authorized Member**” means a Member who is authorized by the Alliance to use the Core Commercial Services and is a party to this Member Services Agreement, or terms substantially similar thereto.

“**Brokered Query Transaction**” means a single document query by an Authorized Member or a Customer.

“**CSA**” shall have the meaning set forth in the Background section of this Agreement.

“**Core Commercial Services**” means the technology services provided by Service Provider to enable patient registration and enrollment, and linking clinical patient records across healthcare organizations for patient identity and consent management described in the Alliance Specifications, together with the querying and retrieval of clinical healthcare record documents then indexed for a patient and available through the network as described in the Alliance Specification, in both cases as the Alliance Specification is amended from time to time. For the avoidance of doubt, Core Commercial Services does not include any of the following services to the extent such services are not dependent upon such Core Commercial Services for: (i) Implementation Services, (ii) data migration services, (iii) provision of patient enrollment, patient matching or document query and retrieval services, or (iv) any patient record matching or document retrieval conducted for purposes of

determining insurance coverage eligibility, payment or claims management.

“**Confidential Information**” means non-public information, including technical, marketing, financial, personnel, planning, and other information that is marked confidential or which the receiving Party should reasonably know to be confidential. Without limitation, Confidential Information may include Data, Member Solution, Member Materials, Service Provider Materials, Service Provider Interfaces, object code, and source code. Confidential Information will not include: (a) information lawfully obtained or created by the receiving Party independently of the disclosing Party’s Confidential Information without breach of any obligation of confidence, (b) information that enters the public domain without breach of any obligation of confidence, (c) Protected Health Information or PHI, the protection of which will be governed by **Exhibit B**, (d) information disclosed for unrestricted release with the written approval of the disclosing Party, or (e) information the receiving Party is obligated to disclose by order or regulation of any governmental entity; provided, however, the receiving Party has given timely notification, to the extent it is reasonably permissible under the circumstances, to the disclosing Party prior to the date of disclosure and the receiving Party uses commercially reasonable efforts to obtain confidential treatment of such information.

“**Customer**” means the specific Member customer(s) that will utilize the Core Commercial Services.

“**Data**” means the electronic information and files that the Member delivers to Alliance through the Core Commercial Services, excluding PHI.

“**Documentation**” means user documentation developed by Service Provider, namely, guidelines and information that describes processes and procedures related to use of the Core Commercial Services, including without limitation protocols around user authorizations and access and other measures that facilitate enhanced protections for the network accessing and using the Core Commercial Services, and developer guides or operating manuals containing the functional

specifications for the Core Commercial Services and that Service Provider provides to Alliance and Members, as may be reasonably modified from time to time by Service Provider.

“**End User Terms**” means the End User Terms and Conditions set forth in Exhibit A-2.

“**Enrollment Transaction**” means a single transaction to enroll a patient by an Authorized Member or a Customer.

“**Force Majeure Event**” means any cause beyond the reasonable control of a Party that could not, by reasonable diligence, be avoided, including acts of God, acts of war, terrorism, riots, embargoes, acts of civil or military authorities, denial of or delays in processing of export license applications, fire, floods, earthquakes, accidents, or strikes.

“**Implementation Services**” means the services provided to optimize the Core Commercial Services and/or Member Interface for use in the Customer’s clinical environment.

“**Independent Member IP**” shall mean all embodiments of Intellectual Property Rights (and the Intellectual Property Rights therein) owned, created or reduced to practice by such Member prior to the execution of this Agreement, or independently of the activities set forth in this Agreement.

“**Individual**” shall have the meaning given to that term by the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations (“HIPAA”).

“**Intellectual Property Rights**” means all forms of legal rights and protections in any country of the world regarding intellectual property rights, including all right, title and interest arising under common and statutory law to all: (i) letters patents, provisional patents, design patents, PCT filings, algorithms, other industrial property rights and other rights to inventions or designs; (ii) trade secret and equivalent rights in confidential or proprietary information and know-how; (iii) copyrights, mask works, moral rights or other literary property or author’s rights; (iv) rights regarding trade names, logos, domain names, URLs, trademarks, service marks and other proprietary indicia or addresses and all goodwill associated therewith; (v) any similar,

corresponding or equivalent rights relating to intangible intellectual property; and (vi) all applications, registrations, issuances, divisions, continuations, continuations-in-part, renewals, reissuances and extensions of the foregoing.

“**Login Credentials**” means unique user identification and password combination, as well as any other applicable security measures that are required by Service Provider to allow Member, a Customer or a User to gain access to the Core Commercial Services.

“**Malicious Code**” means any viruses, worms, unauthorized cookies, trojans, malicious software, “malware” or other program, script, routine, subroutine or data that either (i) disrupts, or is designed to disrupt, the proper operation of the system or device into which it is introduced, the Core Commercial Services (or any part thereof), or any hardware or software of Service Provider, Alliance, a Member or a Customer, or (ii) upon the occurrence of an event, the passage of time or the taking of or failure to take any action, shall cause or result in a system, device, the Core Commercial Services (or any part thereof) or any hardware, software, or data used by Service Provider, Alliance, a Member or a Customer to be improperly accessed, destroyed, altered, damaged or otherwise made inoperable or unreadable.

“**Membership Agreement**” means the CommonWell Health Alliance Membership Agreement adopted by the Alliance on October 7th, 2013.

“**Member Interface**” means the software integrated with the applicable Member Solution to allow the exchange of data uni-directionally or bi-directionally with the Core Commercial Services in accordance with the Alliance Specification and the interface specifications for any Data or PHI originating from and unique to Member systems or the Customer’s system, as well as the software integrated with the applicable Member Solution to exchange Data and PHI with other Companies.

“**Member Materials**” means (a) Independent Member IP, (b) Member and Customer business requirements, work-flows, and operational processes (“Member Processes”) and the Member Interfaces and related materials, concepts and



inventions in the Member Processes and Member Interfaces created by Member whether before, on or after the Effective Date, and (c) all modifications and derivative works of the foregoing.

“**Member Solution**” means the applicable Member electronic medical record solution or healthcare information technology solution that manages patient related data for such Member.

“**Party**” or “**Parties**” references party or both Member and Alliance.

“**Protected Health Information**” or “**PHI**” will have the same meaning as the term “protected health information” in 45 C.F.R. § 160.103, as applied to the information created, received, maintained or transmitted by Service Provider or on behalf of Alliance or a Member.

“**Service Provider Interface**” means the application program interfaces that Service Provider makes available to Alliance, Member or Customers in connection with accessing or exchanging data with the Core Commercial Services.

“**Service Provider Materials**” means (a) the Independent Service Provider IP, Core Commercial Services and Service Provider Interfaces and related materials, concepts and inventions created by Service Provider whether before, on or after the Effective Date, (b) all other tools, utilities, methodologies, templates and processes developed or owned by Service Provider, and (c) all modifications and derivative works thereof.

“**Services**” means the Core Commercial Services and any other services that Service Provider provides to Member, and/or Customers under this Agreement including without limitation Implementation Services, support services and data migration services.

“**Service Provider**” means the Service Provider retained by the Alliance to provide the Core Commercial Services.

“**Specification**” means each document designated as a “CommonWell Health Alliance Specification” as finally adopted and approved by the Board of Directors pursuant to the Bylaws.

“**Third Party Materials**” means the data and software owned by third parties provided by Service Provider, Alliance or a Member under this Agreement.

“**Transaction**” means the combination of a Brokered Query Transaction and an Enrollment Transaction.

“**Use**” means any access, creation, receipt, maintenance, transmission, use or disclosure.

“**User**” means any individual user (including a physician or any other individual) of the Core Commercial Services authorized to use the Core Commercial Services. Users may be employed by Member or a Customer, or affiliated with Member or a Customer, but in all cases shall be authorized by Member to use the Core Commercial Services.

EXHIBIT A-2
COMMONWELL HEALTH ALLIANCE
MEMBER SERVICES AGREEMENT (MSA) EULA

Background and Purpose

This CommonWell Health Alliance (“Alliance”) Member Services Agreement (“MSA”) End User License Agreement (“EULA”) applies to and is incorporated in its entirety by reference into the MSA. The MSA is required in order for a Member to receive the Services. Member must pass through to its Customers terms substantially similar to the following, if Member distributes or sublicenses the rights to receive the Services to its Customers:

Terms and Conditions

1. Description of Services. Customer acknowledges and agrees that, as part of the Services, Health Data of Customer and each of its End Users may be used and disclosed by Alliance through its Service Provider and disclosed to other Members’ Customers and End Users participating in the Services, solely as necessary to provide the Services, as further described below. Customer represents and warrants that it has all rights and authority necessary to agree to and comply with the previous sentence and all Health Data provided to Alliance or Service Provider or exchanged via the Services by Customer and its End Users is provided with the full authority and consent of the owner of such Health Data as set forth in Section 4 of this EULA.

Health Data may be used and disclosed by Alliance and Service Provider and their subcontractors solely as necessary to provide the Services, including on behalf of Customer or End Users to carry out the following related to the Services: (a) submit requests for Health Data relating to individual patients, (b) identify whether other participants utilizing the Services maintain Health Data relating to those patients, (c) request Health Data from the participants maintaining it, (d) transmit requested Health Data to the requesting participant, and in support of other uses approved by the Alliance. In addition, Alliance and Service Provider may de-identify PHI and store Health Data and de-identified PHI for the sole purposes of performance testing, trouble shooting and improving the Services within the scope of the MSA, and for no other purpose.

2. Licenses. Customer hereby receives a limited, nonexclusive, non-transferable, non-sublicensable license to access the Services as integrated with and accessible via a designated Customer healthcare information technology solution, solely for Customer’s internal purposes, and only for purposes approved by the Alliance.

3. Access to Services. The Services include the login features described in the Documentation. Each End User will be required to enter his or her login credentials (“Login Credentials”) in order to access the Services. Customer is fully responsible for all uses of Login Credentials issued to or created by its End Users. Customer is responsible for authentication and identity management of each End User that accesses the Services and to ensure such Login Credentials are unique to each End User and remain secure. Customer shall ensure that each End User accessing clinical data using the Services is properly identified, authenticated and authorized under applicable law to access such Health Data.

4. Authority and Consent. Customer agrees to use or disclose data received from other participants in the Services responsibly and in accordance with Applicable Laws, including but not limited to any and all required consents. Customer shall ensure, and train and obligate its Ends Users to ensure, that patient consents are: (i) made with full transparency and education; (ii) adequate to allow all Services approved by the Alliance (iii) made only after the patient has had sufficient time to review educational material; (iv)

commensurate with circumstances for why health information is exchanged; (v) not used for discriminatory purposes or as a condition for receiving medical treatment; (vi) consistent with patient expectations; and (vii) revocable at any time. Customer agrees, and shall cause and obligate each End User to agree, that it shall access and use Health Data only for purposes approved by Alliance.

5. Business Associate Agreements. Customer represents and warrants that it has and will maintain a business associate agreement in conformance with Applicable Laws with Member that is applicable to and covers the use and disclosure of Health Data for participation in the Services.

6. Suspension of Services. Alliance, Service Provider, and Member each retain the right to suspend the Services provided to Customer at any time in the event that Customer is not in material compliance with this EULA or to protect the performance, integrity and security of the Services.

7. PHI Accuracy and Completeness. Each Customer agrees and will require its End Users to agree to the following terms, or to terms substantially similar thereto:

7.1 Alliance through Service Provider provides the technology and services to allow Customer (and its respective Users) to request and disclose their PHI, and as such, Alliance and Service Provider give no representations or guarantees about the accuracy or completeness of the PHI disclosed through the Services;

7.2 PHI disclosed or received using the Services may not be a complete clinical record or history with respect to any individual, and it is the sole responsibility of any treating healthcare provider to confirm the accuracy and completeness of any PHI or clinical records used for treatment purposes and to obtain whatever information the provider deems necessary for the proper treatment of the patient;

7.3 Customer and each of its End Users is solely responsible for any decisions or actions taken involving patient care or patient care management, whether or not those decisions or actions were made or taken using information received through the Services; and

7.4 Alliance and Service Provider assume no responsibility or role in the care of any patient.

8. Compliance with EULA and Alliance Policies. Customer agrees (i) to utilize the Services in accordance with the terms and conditions of this EULA, and (ii) to comply with and to obligate its End Users to comply with all Alliance Policies, and (iii) to provide reasonable training to End Users regarding the use of the Services in accordance with the terms and conditions of this EULA, Alliance Policies, and Documentation.

9. Carequality Services. Services may include products and services to Customers which involve access to, use of, and re-disclosure of Information that the Alliance obtains by virtue of being an Carequality Implementer (“Carequality Services.”). If Customer has access to or uses Carequality Services, Customer hereby agrees that: (i) with regards to such Carequality Services Customer agrees to and shall comply with the Carequality Connection Terms; (ii) acknowledges that the Carequality Connection Terms constitute a binding written agreement between Customer and Alliance, and; (iii) Customer consents and has adequate authority to consent to Customer and its customers to participate in the Carequality Services, including but not limited to any applicable exchange Activity related thereto. “Carequality Connection Terms” means the Carequality terms and conditions, as updated from time to time and available from Carequality here: <https://sequoiaproject.org/>. For the purpose of this Agreement “Carequality Implementer” has the meaning provided in the Carequality Connection Terms.

10. Accuracy and Data Backup. Customer acknowledges and agrees that it is solely responsible for the accuracy of data it provides through the Services and that Alliance and Service Provider are not responsible for the accuracy or content of the data used or disclosed in providing the Services. Customer is responsible for establishing and operating its own back-up, and other procedures and controls appropriate to maintain the integrity and continuity of Customer's operations, including the protection of its data and PHI or of its End Users.

11. Breach Detection and Notification. Customer shall comply with all applicable breach notification requirements pursuant to 45 CFR § 164.410. Customer shall make reasonable efforts to notify Member of any Breach of Confidentiality or Security within three (3) days from discovery.

12. Compliance with Laws. Customer is, and will remain, and will obligate End Users to be and remain, compliant with all Applicable Laws in their use of the Services, including laws that become effective during the use of the Services.

13. Proprietary Rights. Customer acknowledges and agrees, as between Customer, Alliance and Service Provider, Customer is only being granted a limited use right to the Services provided by Alliance or Service Provider. Alliance and Service Provider retain all rights title and interest in and to their own respective Intellectual Property rights. The Services and all additions or modifications to the Services provided by Alliance or Service Provider, and all Intellectual Property rights associated therewith, are the sole and exclusive property of Alliance, Service Provider, or their licensors.

14. LIMITATION OF LIABILITY. IN NO EVENT WILL ALLIANCE OR SERVICE PROVIDER BE LIABLE TO CUSTOMER UNDER, IN CONNECTION WITH, OR RELATED TO THE SERVICES FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, LOST PROFITS OR LOSS OF GOODWILL, WHETHER BASED ON BREACH OF CONTRACT, WARRANTY, TORT, PRODUCT LIABILITY, OR OTHERWISE, AND WHETHER OR NOT ALLIANCE OR SERVICE PROVIDER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. ALLIANCE AND SERVICE PROVIDER'S ENTIRE LIABILITY TO CUSTOMER FOR ANY LOSS OR DAMAGE, DIRECT OR INDIRECT, FOR ANY CAUSE WHATSOEVER AND REGARDLESS OF THE FORM OF ACTION, RELATED TO CUSTOMER'S USE OF THE SERVICES, WILL BE LIMITED TO CUSTOMER'S ACTUAL DIRECT OUT-OF-POCKET EXPENSES WHICH ARE REASONABLY INCURRED BY CUSTOMER IN AN AMOUNT NOT TO EXCEED \$25,000.00.

15. Exclusive Warranty and Disclaimer. ALLIANCE AND SERVICE PROVIDER MAKE NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT, INCLUDING WITHOUT LIMITATION WITH REGARDS TO THE SERVICES.

16. Service Provider as Third Party Beneficiary. Alliance and Service Provider are third party beneficiaries of this EULA and are each entitled to enforce any rights herein that relate to its rights in the Services, including rights related to any Intellectual Property owned by each of them.

Definitions

In addition to terms defined elsewhere in this EULA, the following defined terms shall apply:

"Alliance Policies" means all policies approved by the Alliance relating to the Alliance or the Services, including but not limited to the Data, Security, and Privacy Policy available on Alliance's website, as updated from time to time. (Please see:

<http://www.commonwellalliance.org/data-and-security/>)

“Applicable Laws” means all applicable federal, state, and local laws, including but not limited to privacy laws, HIPAA, and those concerning the use of PHI related to minors, personally identifiable information, and sensitive personal information.

“Breach” has the meaning provided for in 45 CFR 164.402 (Definitions, effective March 26, 2013; 78 Federal Register 5695) or its successor.

“Breach of Confidentiality or Security” means an incident that is reasonably likely to adversely affect: (a) the viability, security, or reputation of the Services, or (b) the legal liability of Alliance, Service Provider, or any Member.

“Customer” means a customer or user of a Member that receives the benefits of the Services.

“Documentation” means the user documentation containing the functional descriptions for the Services as may be reasonably modified from time to time by Alliance or Service Provider.

“End User” means a healthcare provider facility, practice group, or physician (including any individual or legal entity), permitted by an Adopter to access the Services or any enrollment user interface to utilize the Services.

“Health Data” means health information, including information and PHI that is received, transmitted, stored or maintained through the Services.

“HIPAA” means the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations.

“Intellectual Property” means all forms of legal rights and protections in any country of the world regarding intellectual property rights, including all right, title and interest arising under common and statutory law to all: patents, trademarks, copyrights, trade secrets, and other industrial property rights and other rights to inventions or designs, and all applications, registrations, issuances, divisions, continuations, continuations-in-part, renewals, reissuances and extensions of the foregoing.

“Login Credentials” means unique user identification and password combination, as well as any other applicable security measures that are required by Service Provider to allow Member, a Customer or a User to gain access to the Services.

“Member” means legal entity, approved by the Alliance, and which is a party to a valid Alliance Membership Agreement.

“Protected Health Information” or “PHI” has the meaning set forth in 45 C.F.R. 160.103, as applied to the information created, received, transmitted or maintained through the Services.

“Services” means the services approved and offered by or on behalf of the Alliance, including but not limited to those related to patient registration, enrollment, linking, and retrieval of electronic healthcare records. Services may include products and services, which involve access to, use of, and re-disclosure of information that the Alliance obtains by virtue of being a Carequality Implementer.

“Service Provider” means a service provider that provides services relating to the Services on behalf of Alliance.

EXHIBIT A-3
FEE SCHEDULE
FEES/RATES

[Intentionally left blank. For information about pricing please contact info@commonwellalliance.org]

EXHIBIT B
COMMONWELL HEALTH ALLIANCE
DATA PRIVACY AND SECURITY POLICY

Background and Purpose

CommonWell Health Alliance, Inc. (“Alliance”) is committed to defining and promoting a national infrastructure with common standards and policies that promote a vendor-neutral platform to break down the technological and process barriers that currently inhibit effective health data exchange.

We are committed to supporting a robust privacy and security standard for all data exchanges through the Alliance Services. As such, the Services and Alliance Specifications are designed with privacy as a key consideration.

Definitions used in this Policy that are not defined elsewhere in the Policy are defined in the Definitions section.

Application

This Data Privacy and Security Policy (“Policy”) identifies the standards and requirements that are applicable to any party that accesses or uses the Services, including Customers, End Users and Members (each defined below, collectively “Adopters”).

Compliance with Laws

This Policy does not supersede or replace any Applicable Laws, including HIPAA, or any federal or state laws or regulations applicable to Alliance, or any Adopter. In their use of the Services, Adopters represent and warrant that they shall remain compliant with all Applicable Laws related to the use of the Services. All parties are required to enter into Business Associate Agreements with other parties as required by law.

Use and Disclosure of Health Information

Adopters shall request, access, use, and disclose Health Data made available through the Services only in accordance with all Applicable Laws, in compliance with all Alliance Policies, and only as specifically authorized and approved by Alliance, and for no other purposes.

Health Data shall be used by or on behalf of Adopters only as necessary to provide or receive the benefit of the Services, including to carry out the following related to the Services: (a) submitting requests for Health Data relating to individual patients, (b) identifying whether other Adopters maintain Health Data relating to those patients, (c) requesting such Health Data from Adopters maintaining it, (d) transmitting requested Health Data to the requesting Adopters, or (e) as otherwise specifically approved by Alliance, and for no other purposes. In addition, Alliance or Service Provider may de-identify PHI, as defined in 45 CFR § 164.514(b)(1) and 164.514(b)(2), and store Health Data and de-identified PHI for the sole purposes of providing the Services in accordance with the terms of the applicable service agreement between Alliance and Service Provider, and for no other purpose.

Patient Consents and Notification

Adopters are required to obtain all necessary patient consents and authorizations required under Applicable Law. Patient consents must be: (a) made with full transparency and education, (b) made only after the patient has had sufficient time to review any applicable educational material, (c) commensurate with the circumstances for which the Health Data is exchanged, (d) not used for discriminatory purposes or as a condition for receiving medical treatment, (e) consistent with patient expectations, and (f) revocable at any time.

Identity Management and Authentication

Each Adopter is fully responsible for all uses of any applicable Login Credentials issued to it or created by it or its users, and for authentication and identity management of each user accessing the Services on behalf of Adopter, and for ensuring that such Login Credentials are unique to each user, and that such credentials remain secure. Adopters are required to ensure that each of its users accessing Health Data using the Services is properly identified, authenticated and authorized under Applicable Law to access such Health Data.

System and Network Security Requirements

Members are required to maintain a secure information technology environment and to use appropriate technical, administrative and physical safeguards to prevent the use or disclosure of PHI other than as permitted hereunder, including appropriate administrative, physical and technical safeguards that protect the confidentiality, integrity and availability of PHI accessed or disclosed through the Services. Adopters are required to develop, implement, maintain and use the safeguards identified in HIPAA Security Rule, 45 C.F.R. Part 160 and 164, Subparts A and C.

Adopters are required to: (a) connect via secure web services connections or through virtual private **network** (VPN) connection between its local area network (LAN) and the Services, (b) implement, use and maintain commercially reasonable firewall technology, (c) implement, maintain and assume all costs for a business class virus protection solution on the Member's and End User's network and computers, and (d) monitor and investigate potential or actual fraudulent activity that involves the Services.

Breach and Notification

Unless Applicable Laws require earlier notice, Adopters are required to report any Breach or Breach of Confidentiality and Security involving the Services to Alliance no later than three (3) days after the Adopter first becomes aware of such breach.

Prohibited Uses

Adopters shall not use the Services to conduct any business or activity, or solicit the performance of any activity, which is prohibited by or would violate any Applicable Laws, or for purposes that may create civil or criminal liability, including: (a) uses which are defamatory, deceptive, obscene, or otherwise inappropriate; (b) uses that violate or infringe upon the rights of any other person, such as unauthorized distribution of copyrighted material; (c) "spamming," sending unsolicited bulk e-mail or other messages using the Services or sending unsolicited advertising or similar conduct; (d) threats to or harassment of another; (e) impersonating another person or other misrepresentation of source; (f) copying, selling, reselling or exploiting any portion of the Services, including Health Data, except as expressly permitted by Alliance; and (g) assisting or permitting any persons in engaging in any of the activities described in this paragraph. Adopters shall not expose or introduce or facilitate the exposure or introduction of any Malicious Code into the Services, or any Alliance system or network, or the systems or networks of any Adopter.

Definitions

In addition to terms defined above, capitalized terms in this Policy have the following meanings:

“Alliance Policies” means all policies approved by the Alliance relating to the Alliance or the Services.

“Alliance Specification” means each document designated as a “CommonWell Health Alliance Specification” as finally adopted and approved by the Alliance.

“Applicable Laws” means all applicable federal, state, and local laws, including but not limited to privacy laws, HIPAA, and those concerning the use of PHI related to minors, personally identifiable information, and sensitive personal information.

“Breach” has the meaning provided for in 45 CFR 164.402 (Definitions, effective March 26, 2013; 78 Federal Register 5695) or its successor.

“Breach of Confidentiality or Security” means an incident that is reasonably likely to adversely affect: (a) the viability, security, or reputation of the Services, or (b) the legal liability of Alliance or any Adopter.

“Customer” means a customer or user of a Member that receives the benefits of the Services.

“End User” means a healthcare provider facility, practice group, or physician (including any individual or legal entity), permitted by an Adopter to access the Services or any enrollment user interface to utilize the Services.

“Health Data” means health information, including information and PHI that is received, transmitted, stored or maintained through the Services.

“HIPAA” means the Health Insurance Portability and Accountability Act of 1996 and its implementing regulations.

“Malicious Code” means any viruses, worms, unauthorized cookies, trojans, malicious software, malware or other program, script, routine, subroutine or data that may disrupt, or is designed to disrupt, the proper operation of software, hardware, networks or systems.

“Member” means a means legal entity, approved by the Alliance, and which is a party to a valid Alliance Membership Agreement.

“Protected Health Information” or “PHI” has the meaning set forth in 45 C.F.R. 160.103, as applied to the information created, received, transmitted or maintained through the Services.

“Service Provider” means a service provider that provides services relating to the Services, on behalf of Alliance.

“Services” means the services approved and offered by or on behalf of the Alliance, including but not limited to those related to patient registration, enrollment, linking, and retrieval of electronic healthcare records.

EXHIBIT C-1
SERVICE PROVIDER - SERVICE LEVEL AGREEMENT

1. Service Level Agreement by Service Provider.

Alliance (through its Service Provider) will provide the Core Commercial Services to Member with an Uptime (as defined herein) of at least ninety-nine point nine percent (99.9%) of Service Provider Available Time (as defined herein) for Core Commercial Services. All service levels shall be measured in the aggregate across all Authorized Members for purposes of determining service level standards. "Uptime" means all times when the Transactions are running and are available to be accessed by each Authorized Member and its Customers as measured by automated site monitoring software operated by Service Provider ("Monitoring Software"). "Service Provider Available Time" means the number of hours in any given period less the amount of Downtime related to (i) Standard Maintenance Window, (ii) scheduled downtime, (iii) internet-wide disruptions, (iv) an Authorized Member or any Customer's use of the Core Commercial Services that is not in accordance with the Alliance Specification (v) any failure of power, environmental systems, networking infrastructure or any other such system at an Authorized Member's or any Customer's facilities or (vi) Downtime otherwise attributable to Alliance, an Authorized Member or any Customer. "Downtime" means all times in which the Core Commercial Services fails HTTP checks, content verification checks, and a service check as measured by the Monitoring Software. "Standard Maintenance Window" means a weekly maintenance period between 10:00 PM and 2:00 AM Pacific time every Tuesday and a second optional period between 6:00 PM Saturday and 2:00 AM Sunday, or as may be scheduled from time to time with fourteen days prior notice to Alliance or an Authorized Member or other emergency maintenance notified to Alliance or an Authorized Member's account representative with at least two hours' notice. Service Provider will provide Alliance and Member a monthly report (which may be provided electronically) by the fifteenth day of each month regarding Service Provider service level performance for the preceding month.

2. Service Level Warranty.

If, per the Monitoring Software, Service Provider breaches the service level to Member as set forth in Section 1 above for any calendar quarterly period, Service Provider will be required to provide Member and the Alliance a detailed report including a root cause analysis and a remediation plan in a timely manner. If the Uptime is below ninety-nine point seven percent (99.7%), Service Provider will provide a credit against fees payable by the impacted Authorized Member(s) to Service Provider the following quarter equal to one percent (1%) of fees payable for that next quarter for each one-tenth of one percent (0.10%) below ninety-nine point seven percent (99.7%) of Uptime. In further consideration, if the Uptime is below ninety-nine percent (99%) for two consecutive calendar quarterly periods, Service Provider will provide a credit against fees payable by the impacted Authorized Member(s) to Service Provider the following quarter equal to ten percent (10%) of fees payable during that next quarter. This paragraph sets forth Service Provider's entire obligation and liability to Member and Member's sole and exclusive remedy for any inability to access or use the Core Commercial Services.

EXHIBIT C-2
SUPPORT SERVICES AND RESPONSIBILITY MATRIX

A. **Summary of Obligations.** The table below summarizes some of the key responsibilities of Member and the Alliance (through its Service Provider).

	Member Responsibilities	Service Provider Responsibilities
Sales and Marketing		
1. Promptly advise Service Provider concerning any charges, complaints, or claims by Customers or others about the Core Commercial Services and any market information that may come to Member's attention regarding the Core Commercial Services and the continued competitiveness of the Core Commercial Services in the marketplace.	√	
2. Service Provider will promptly advise Member of any charges, complaints, or claims regarding the Member's performance related to the Core Commercial Services during the Term		√
3. Maintain the ability to effectively demonstrate the Core Commercial Services	√	
4. Contract with Customers for Core Commercial Services	√	
Implementation		
5. Software installation at the Customer site	√	
6. Train Member on the process to deploy and provide Customer training for the Core Commercial Services		√
7. Provide Customer training to support full Customer participation	√	
8. Have personnel trained by Service Provider on staff	√	
9. Setup and configuration of Customer systems and users on the Core Commercial Services	√	
10. Daily monitor transmission and response files and inform Service Provider of any irregularities provided the timing of such information may be adjusted for circumstances outside of Member's control	√	
11. Provide onboarding process for Customers with respect to the Core Commercial Services	√	
Support		
12. Provide Tier I & Tier II Support for Customers with respect to the Core Commercial Services	√	
13. Provide support to Member with respect to the Core Commercial Services, including promptly providing all error corrections and updates		√
14. Provide status updates and communication to Customers on reported issues	√	
15. Provide Service Provider with troubleshooting steps and data on Customer issues that are escalated to Service Provider	√	
16. Provide training on Core Commercial Services to Member Support		√

	Member Responsibilities	Service Provider Responsibilities
Representatives.		
17. Provide Tier III Support for issues reported to Service Provider		√
18. Provide status updates and communication to Member on reported issues		√

B. Implementation and Delivery Services.

1. **Overview.** Member is responsible for providing its Customers with the required Implementation Services associated with the Core Commercial Services.
2. **Implementation Delivery and Issues Reporting.** Member will have responsibility for implementing the Core Commercial Services and supporting its Customers(s) while implementing the Core Commercial Services. Service Provider will maintain responsibility for supporting Member in resolving Core Commercial Services issues during the implementation process. Member will maintain the relationship with its Customers. In addition to the guidelines and requirements set forth in the Implementation Plan, the following apply:
 - a) Member will be the primary contact for all Customer implementation issues during the implementation process. Member will provide Tier I and Tier II support for those issues. Member will escalate Tier III issues related to the Core Commercial Services to Service Provider’s support team (“**Service Provider Support**”) via the Alliance support email address with details of issue that fully describes the incident and the efforts undertaken by Member to resolve the problem, unless an alternate means of communication related to escalation is otherwise mutually agreed upon in writing.
 - b) Service Provider Support will be responsible for adhering to the issue prioritization and response time goals in continuing with the resolution process and maintaining communication and updates back to the Member.
 - c) To facilitate coordination and resolution of Customer issues, Service Provider will use the contact information in the Member’s case reporting system and the Member will access the published Contact List from Service Provider. This Contact List will be made available on the Alliance extranet and will be updated monthly by Companies and Service Provider support leadership.
 - d) Member will deliver to Service Provider an electronic copy of demographic data from the Member systems for the Customers participating in the Core Commercial Services.
 - e) Member will facilitate a regular patient identity demographic information feed from Customer to Service Provider to assist in maintaining the effectiveness of the Core Commercial Services.
3. **Issue Management Responsibilities**
 - a) Member will be responsible for initial intake and triage of Customer calls and reporting to Service Provider Support. Member will direct Customers to follow standard procedures for issue reporting during implementation.
 - b) If Member is unable to resolve the issue, Member will escalate the issue to Service Provider Support via email at support@commonwellalliance.org. or other communication method as mutually agreed. For Critical Severity Issues or High Severity Issues (defined herein), if an alternate means of communication related to escalations is not otherwise mutually agreed and established, Member will follow up with a phone call to inform Service Provider Support of the severity level. Member will retain responsibility of Customer interactions and communications.

- 1) Member will gather the data below and include as part of the initial email to support@commonwellalliance.org, as applicable:
 - a. Member case number
 - b. Case Severity Level (Critical, High, Medium, Low)
 - c. Member Customer
 - d. Member contact name(s) and email/phone number
 - e. Environment (i.e. Production, Test)
 - f. Issue description (add applicable information):
 - i. Description of the issue
 - ii. Is the issue reproducible?
 - iii. Patient and data and example (service called, expected vs. actual data returned)
 - iv. Is the issue affecting an individual user, a hospital, a practice, or an entire group?
 - v. Any log files or errors that can be provided from the transaction
 - vi. Summary of Member issue resolution efforts
 - 2) Service Provider Support will generate a support case from the initial email and respond back to Member contacts noted in the initial email, with a case number within time frames defined below.
 - 3) Service Provider Support will assign and work the issue according to issue severity level. Service Provider Support will provide status updates on the case.
 - a. If issue is setup related, Service Provider will communicate back to Member with the correct procedure that will resolve the issue so Member can track/train in their knowledge base and implement resolution with the Customer.
 - b. If the issue is a defect, Service Provider will use the originating tracking number for status updates.
 - 4) If Service Provider Support needs to contact Member for escalation or consultation, Service Provider will contact Member, and Member will open a case or update an existing case at that time. Escalation roles are identified above. The escalation contact name and contact information can be found on the contact list for Member on the contact list published on the Alliance Extranet.
- c) If a Customer contacts Service Provider Support directly to report an issue, Service Provider Support will inform the Customer that they should contact Member with the issue and submit a case if they have not already done so. Service Provider will assist the Customer by providing contact information to Member Support contact listed on the Alliance Extranet.

C. Support Services

- a. **Overview.** During the term of this Agreement, Service Provider will provide the Core Commercial Services to all Authorized Members to assist in the interoperability between the Member Solutions. As a result, Member may identify certain issues or bugs that are outside the control of Service Provider. In such case, Service Provider will endeavor to enable a structure by which Member can escalate and track issues or bugs among one another, but Service Provider will not be responsible for resolving or facilitating the resolution of such issues or bugs.
- b. **Customer Support and Issues Reporting.** Member will maintain responsibility for supporting Customers using the Member Solution and other Authorized Member systems. Service Provider will maintain responsibility for supporting Member in resolving Customer issues with the Core Commercial Services. Member will retain ownership of the Customer. The following guidelines apply:

- i. Member will be the primary contact for all Customer issues relating to the Member Solution and other Member systems and will provide Tier I and Tier II support for those issues. Member will escalate Tier III issues related to the Core Commercial Services via the Alliance support email address with details of issue that fully describes the incident and the efforts undertaken by the Member team to resolve the problem.
 - ii. Service Provider Support will be responsible for adhering to the issue prioritization and response time goals in continuing with the resolution process and maintaining communication and updates back to the Member.
 - iii. To facilitate coordination and resolution of Customer issues, Service Provider and Member shall publish and maintain a key contact list.
- c. Customer Support Responsibilities.**
- i. Member will be responsible for initial intake and triage of Customer calls and service orders. Customers will be directed to contact Member Support.
 - ii. If Member is unable to resolve the issue, Member will escalate the issue to Service Provider Support through the following method, as applicable:
 - 1. Via email at support@Commonwellalliance.org
 - 2. For critical/high issues, follow up with a phone call to inform Service Provider Support of the Severity Level.
 - 3. Member will retain ownership of Customer service order, Customer interactions and Customer communication.
 - 4. Service Provider Support will generate a support case from the initial email and respond back to Member with a case number within time frames defined below.
 - d. If issues reported to Service Provider require the coordination of multiple Members to resolve, Service Provider Support will facilitate the coordination of necessary parties to reach resolution.
 - e. If Customers contact Service Provider support directly to report an issue, Service Provider Support will inform the Customer that Member Support should be contacted first and assist the Customer by providing contact information to the Member Support contact listed on the Alliance Extranet.

D. Support Services, Business Hours, and Support Tiers

a. Support Services

Severity	Definition	Example	Support Assignment SLA
1-Critical	An issue resulting from an inability to access core CommonWell services from multiple organizations or a large group of users.	<ul style="list-style-type: none"> • Workflow Initiating APIs not available (patient Match, Search Person) over a sustained length of time (greater than 15 minutes) • Entire Organization (HomeCommunityID) unable to access CommonWell Services. This could be due to a Certificate being invalid. This would only apply to an Organization that was previously configured and working properly. Not initial setup and configuration of a new Organization. 	Assignment within 1 hour with communication every hour until resolution or agreed timeframe between Members and Service Provider Support. Intensity 24x7. NOTE: The 1 hour assignment time will be reviewed over the next couple months with the intent to reduce this once the appropriate teams and training is in place.
2-High	An issue that is affecting only a subset of users or CommonWell functionality. There is no workaround.	<ul style="list-style-type: none"> • Unusual slow system performance • A small subset of users is unable to access workflow 	Assignment less than 1 Business Day with daily follow-up or other agreed upon timeframe. Intensity normal business hours.

		<p>initiating APIs (patient match, person Search) over a sustained length of time (greater than 15 minutes)</p> <ul style="list-style-type: none"> • Single or Multiple service calls are always failing for a subset of users. • Issue is preventing customer from completing key implementation task(s) in the designated time • A New or Update organization Request 	
3-Medium	<p>An issue that affects customer usage or data integrity. There is a workaround. Set up, training, testing and Customer Education, can continue as scheduled during an implementation. If the customer is live Medium issues may relate to problems in Productions, Test, QA or Training environments. Project Requests and Organization Requests fall under Medium Severity.</p>	<ul style="list-style-type: none"> • Product, Service or documentation contains incorrect logic, incorrect descriptions, or functional problems which the customer is able to work around or where a temporary correction has been implemented (fully functional but needs improvement). • Single or Multiple service calls are occasionally failing for a subset of users. • A single document source is unavailable or returning invalid data over an extended period of time based on an unplanned outage. 	<p>Assignment in less than 5 Business Days with follow-up every 3 days or other agreed upon timeframe. Intensity normal business hours.</p>
4-Low	<p>A low impact issue which could be a question or concern about the way CommonWell behaves in a specific scenario but the answer is not needed in an urgent manner.</p>	<ul style="list-style-type: none"> • Service is responding as expected but there is a question about why it responds that way. • A single document source is unavailable or returning invalid data over an extended period of time based on a planned outage. 	<p>Assignment in less than 10 Business Days with follow-up every 5 days or other agreed upon timeframe. Intensity normal business hours.</p>

b. Business Hours. Member and Service Provider agree to the following definition of Business and After Hours:

- i. Member Business Hours: Support provided for all priorities Monday thru Friday, 7am to 5pm Mountain Time Zone.
- ii. Member After Hours and Holidays: Support provided for Critical Severity Issues Monday through Thursday and weekends outside of RH Business hours below. After Hours and Holiday issues will follow the Member After Hours issue escalation and handling process.
- iii. Service Provider Business Hours: Support provided for all priorities Monday through Friday 7am to 5pm Mountain Time Zone.
- iv. Service Provider After Hours and Holidays: Support provided for Critical priority issues outside of RH Business Hours above. (M-F 7-5 Mountain Time Zone).

c. Support Tiers.

- i. Tier I – Member Support analysts, application and technical support for Member related application, setup and connection issues.

- ii. Tier II – Member Support product and technical advisors, subject matter experts for Member related application, setup and connection issues.
- iii. Tier III – Service Provider Support for non-Member related application, setup and connection issues.

EXHIBIT D

IMPLEMENTATION PLAN

Key Activities	Descriptions	Expected Duration & Timeline (weeks)	CommonWell Resources	
			Member	Service Provider
PROJECT PREREQUISITES				
Non- Technical Confirmation of resource commitment	Customer expectations & requirements to be confirmed to ensure customers can engage in implementation. Note: Some technical prerequisites identified may not apply to all Members and Customers. The Members will use either the ELC App or provide a functional equivalent.	2 Weeks	Project Manager, Technical Team	Project Manager, Technical Team
Technical 1. Code release version 2. Software Packages 3. Software components 4. Security Certificates requirements 5. Hardware requirements 6. Backload requirements 7. ELC App requirements 8. Customer's Software Requirements				
PROJECT KICKOFF ENGAGEMENT				
Discuss Project Scope	Review implementation logistics as they relate to and impact timelines, practice workflow and provider/patient impact.	2 Weeks	Project Manager, Product Manager if not included in the "Technical Team," Technical Team	Project Manager
Discuss Project Timeline				
Discuss Workflow Impact				
Discuss Patient Impact				
SYSTEM CONFIGURATION				
Perform technology assessment	Complete technical project planning, technical configuration, and unit testing to confirm connectivity is established in preparation for end-to-end testing.	3 Weeks	Project Manager, Technical Team	Project Manager
Evaluate hardware readiness				
Develop interface triggers				
Establish connections (INT, PROD)				
SYSTEM VALIDATION / TESTING				

Key Activities	Descriptions	Expected Duration & Timeline (weeks)	CommonWell Resources	
			Member	Service Provider
Availability of test environments	Confirm testing requirements are in place to begin end-to-end testing. Utilize test plan provided to conduct testing validation. Report out issues/bugs for review and follow up.	4 Weeks	Project Manager, Technical Team	Project Manager, Technical Team
Create test patients				
Validate test patients				
Test Connectivity (INT, PROD)				
Develop testing plan				
Execute test plans				
Certification				
TRAINING				
Identify super users	Complete production readiness with training of identified users. Customized training will be provided based upon workflow impact during deployment.	3 Weeks	Project Manager, Technical Team, QA Team	Project Manager, Technical Team, Support Team
Provide training – use of Management portal to identify and troubleshoot issues and problems – to Member for end user support				
Modify training curriculum & materials				
Provide end user training			N/A	
CONVERSION				
Validate production operation	Turn production feeds on; Alliance members will monitor production interfaces and triage issues identified through Support model.	1 Week	Project Manager, Technical Team, Support Team	Project Manager, Technical Team, Support Team
Turn Live Feed on				
Go-Live				
Turn over to Support – Member will also train its own development teams to self service, troubleshoot, and resolve	Transition production feeds to Customer Support.	TBD by Member		
POST CONVERSION MONITORING AND IMPROVEMENT				
Begin customer support (1st, 2nd, 3rd Levels)	Post Go-Live monitoring for process/technical improvement	Ongoing	Project Manager, Support Team	Project Manager, Support Team
Begin ongoing reporting and monitoring				
Perform post conversion review				

EXHIBIT E
BUSINESS ASSOCIATE ADDENDUM
ALLIANCE-MEMBER

This business associate agreement (this “BAA”) applies to the PHI received, created, maintained or transmitted by Alliance in providing the following business associate services in connection with the CommonWell Health Alliance Core Commercial Services (as such term is defined in the Underlying Agreement) to Member:

1. Maintenance, use and disclosure of PHI by Alliance on behalf of Member in providing the Core Commercial Services.
2. Receipt of PHI by Alliance from Member, receipt of requests for PHI by Alliance from Member with respect to specific patients, submission on behalf of Member of those requests to other participating vendors/providers, receipt on behalf of Member of responses from other participating vendors/providers to Member requests, and provision to Member of those responses.

SECTION 1: DEFINITIONS

“**Breach**” will have the same meaning given to such term in 45 C.F.R. § 164.402.

“**Covered Entity**” will have the same meaning given to such term in 45 C.F.R. § 160.103.

“**Designated Record Set**” will have the same meaning as the term “designated record set” in 45 C.F.R. § 164.501.

“**Electronic Protected Health Information**” or “**Electronic PHI**” will have the meaning given to such term under the Privacy Rule and the Security Rule, including, but not limited to, 45 C.F.R. § 160.103, as applied to the information that Alliance creates, receives, maintains or transmits from or on behalf of Member.

“**Individual**” will have the same meaning as the term “individual” in 45 C.F.R. § 160.103 and will include a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).

“**Parties**” will mean, collectively, Member and Alliance.

“**Party**” will mean, individually, Member or Alliance.

“**Privacy Rule**” will mean the Standards for Privacy of Individually Identifiable Health Information at 45 C.F.R. Parts 160 and Part 164, Subparts A and E.

“**Protected Health Information**” or “**PHI**” will have the same meaning as the term “protected health information” in 45 C.F.R. § 160.103, as applied to the information created, received, maintained or transmitted by Alliance from or on behalf of Member or its Customers. All references to PHI include Electronic PHI.

“**Required by Law**” will have the same meaning as the term “required by law” in 45 C.F.R. § 164.103.

“**Secretary**” will mean the Secretary of the Department of Health and Human Services or his or her designee.

“**Security Incident**” will have the meaning given to such term in 45 C.F.R. § 164.304.

“**Security Rule**” will mean the Security Standards at 45 C.F.R. Parts 160 and Part 164, Subparts A and C.

“**Unsecured PHI**” will have the same meaning given to such term under 45 C.F.R. § 164.402, and guidance promulgated thereunder.

“**Underlying Agreement**” will mean the Member Services Agreement between Alliance and Member.

Capitalized Terms. Capitalized terms used in this BAA and not otherwise defined herein will have the meanings set forth in the Privacy Rule, the Security Rule, and the HIPAA Final Rule, and the Underlying Agreement which definitions are incorporated in this BAA by reference.

SECTION 2: PERMITTED USES AND DISCLOSURES OF PHI

2.1 Uses and Disclosures of PHI Pursuant to the Underlying Agreement. Except as otherwise limited in this BAA, Alliance may use or disclose PHI solely to perform services for Member as specified in the Underlying Agreement, provided that such use or disclosure would not violate the Privacy Rule if done by the Member or a Covered Entity. Alliance may de-identify PHI to performance test, trouble-shoot and improve the Core Commercial Services as provided in the Underlying Agreement. Except as set forth in the prior sentence, in no event may Alliance de-identify or aggregate PHI or Electronic PHI or use or disclose any PHI or Electronic PHI for data mining, to provide data aggregation services or to develop new products or services.

2.2 Permitted Uses of PHI by Alliance. Except as otherwise limited in this BAA, Alliance may use PHI for the proper management and administration of Alliance related to the Core Commercial Services, which is defined as risk management, quality control, and support services for the Alliance infrastructure to provide the Core Commercial Services.

2.3 Permitted Disclosures of PHI by Alliance. Except as otherwise limited in this BAA, Alliance may disclose PHI for the proper management and administration of Alliance related to the Core Commercial Services, which is defined as risk management, quality control, and support services for the Alliance infrastructure to provide the Core Commercial Services, provided that the disclosures are Required by Law, or Alliance obtains reasonable assurances from the person 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 (which purpose must be consistent with the limitations imposed upon Alliance pursuant to this BAA), and that the person agrees to notify Alliance of any instances of which it is aware in which the confidentiality of the information has been breached. Alliance may use PHI to report violations of law to appropriate federal and state authorities, consistent with 45 C.F.R. § 164.502(j)(1). All other uses or disclosures of PHI or Electronic PHI not expressly authorized by this BAA or Required by Law are strictly prohibited.

SECTION 3: OBLIGATIONS OF ALLIANCE

3.1 Appropriate Safeguards. Alliance will use appropriate safeguards and will comply with the Security Rule with respect to Electronic PHI, to prevent use or disclosure of such information other than as provided for by the Underlying Agreement and this BAA. Except as expressly provided in the Underlying Agreement, Alliance shall not assume any obligations of a Covered Entity under the HIPAA Final Rule. To the extent that Alliance is to carry out any of Covered Entity's obligations under the HIPAA Final Rule as expressly provided in the Underlying Agreement, Alliance will comply with the requirements of the HIPAA Final Rule that apply to Member in the performance of such obligation.

3.2 Reporting of Improper Use or Disclosure, Security Incident or Breach. Alliance will report to Member any use or disclosure of PHI not permitted under this BAA, Breach of Unsecured PHI or any Security Incident, without unreasonable delay, and in any event no more than five (5) days following discovery and will provide a further report within a reasonable period of time after the information becomes available using commercially reasonable efforts to do so within ten (10) days following discovery; provided, however, that Member acknowledges and agrees that this Section constitutes notice by Alliance to Member of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined below) for which notice to Member by Alliance will be required only upon request. "Unsuccessful Security Incidents" will include, but not be limited to, pings and other broadcast attacks on Alliance's firewall, port scans, unsuccessful log-on attempts, denials of service and any combination of the above, so long as no such incident results in unauthorized access, use or disclosure of PHI. Alliance's notification to Member of a Breach will include: (i) the identification of each individual whose Unsecured PHI has been, or is reasonably believed by Alliance to have been, accessed, acquired or disclosed during the Breach; (ii) any particulars regarding the Breach that a Covered Entity would need to include in its notification, as such particulars are identified in 45 C.F.R. § 164.404; and (iii) the remedial actions taken by Alliance to mitigate the adverse effects of the Breach.

3.3 Alliance's Agents. In accordance with 45 C.F.R. § 164.502(e)(1)(ii) and 45 C.F.R. § 164.308(b)(2), as applicable, Alliance will enter into a written agreement with any agent or subcontractor that creates, receives, maintains or transmits PHI on behalf of Alliance for services provided to Member, providing that the subcontractor or agent agrees to restrictions and conditions that are substantially similar to those that apply through this BAA to Alliance with respect to such PHI or Electronic PHI.

3.4 Access to PHI. The Parties do not intend for Alliance to maintain any PHI in a Designated Record Set for Member. To the extent Alliance possesses PHI in a Designated Record Set, Alliance agrees to make such information available to Member pursuant to 45 C.F.R. § 164.524, within five (5) business days of Alliance's receipt of a written request from Member; provided, however, that Alliance is not required to provide such access where the PHI contained in a Designated Record Set is duplicative of the PHI contained in a Designated Record Set possessed by Member. If an Individual makes a request for access pursuant to 45 C.F.R. § 164.524 directly to Alliance, or inquires about his or her right to access, Alliance will promptly forward such request to Member.

3.5 Amendment of PHI. The Parties do not intend for Alliance to maintain any PHI in a Designated Record Set for Member. To the extent Alliance possesses PHI in a Designated Record Set, Alliance agrees to make such information available to Member for amendment pursuant to 45 C.F.R. § 164.526 within five (5) business days of Alliance's receipt of a written request from Member. If an Individual submits a written request for amendment pursuant to 45 C.F.R. § 164.526 directly to Alliance, or inquires about his or her right to amendment, Alliance will promptly forward such request to Member.

3.6 Documentation of Disclosures. Alliance agrees to document such disclosures of PHI and information related to such disclosures as would be required for Member to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528. Alliance will document, at a minimum, the following information ("Disclosure Information"): (a) the date of the disclosure; (b) the name and, if known, the address of the recipient of the PHI; (c) a brief description of the PHI disclosed; (d) the purpose of the disclosure that includes an explanation of the basis for such disclosure; and (e) any additional information required under the HITECH Act and any implementing regulations.

3.7 Accounting of Disclosures. Alliance agrees to provide to Member, within ten (10) days of Alliance's receipt of a written request from Member, information collected in accordance with Section 3.6 of this BAA, to permit Member to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528. If an Individual submits a written request for an accounting of disclosures of PHI pursuant to 45 C.F.R. § 164.528 directly to Alliance, or inquires about his or her right to an accounting, Alliance will promptly forward such request to Member.

3.8 Governmental Access to Records. Alliance will make its internal practices, books and records relating to the use and disclosure of PHI received from, or created or received by Alliance on behalf of Member available to the Secretary, and ensure a copy of written materials delivered to the Secretary is delivered to Member, for purposes of the Secretary determining a Covered Entity's or Member's compliance with the Privacy Rule, the Security Rule, and/or the Final Rule.

3.9 Mitigation. To the extent practicable, Alliance will mitigate and cooperate with Member's efforts to mitigate a harmful effect that is known to Alliance of a use or disclosure of PHI by Alliance that is not permitted by this BAA.

3.10 Minimum Necessary. Alliance will request, use and disclose the minimum amount of PHI necessary to accomplish the purpose of the request, use or disclosure, in accordance with 45 C.F.R. § 164.514(d), and any amendments thereto.

3.11 HIPAA Final Rule Applicability. Alliance acknowledges that enactment of the HITECH Act, as implemented by the HIPAA Final Rule, amended certain provisions of HIPAA in ways that now directly regulate, or will on future dates directly regulate, Alliance under the Privacy Rule and Security Rule. Alliance agrees to comply with applicable requirements imposed under the HIPAA Final Rule, including any amendments thereto.

3.12 In the event that a Breach is identified and it is determined that, (i) individual and/or public notification is required and (ii) that the requirement for notification is due to the acts or omissions of Alliance, its subcontractors or

agents, Alliance shall be responsible for the reasonable and necessary costs incurred by Member to meet all federal and state legal and regulatory disclosure and notification requirements including but not limited to costs for investigation, risk analysis, any required individual and/or public notification, fines and mitigation activities.

3.13 Reasonable Assurances. Upon reasonable written request of Member, Alliance will provide Member with reasonable assurances that Alliance is in compliance with the obligations of this BAA. Such assurances may include, without limitation, information from third party consultants or security reviews, or, as mutually agreed upon with Alliance, a third party audit of the Alliance information technology used to provide the Core Commercial Services.

SECTION 4: PERMISSIBLE REQUESTS BY MEMBER

4.1 Permissible Requests by Member. Member will not request Alliance to use or disclose PHI in any manner that would not be permissible under the Privacy Rule, the Security Rule or the HITECH Act if done by Member, except as permitted pursuant to the provisions of Sections 2.2 and 2.3 of this BAA.

SECTION 5: TERM AND TERMINATION

5.1 Term. The term of this BAA will commence as of the BAA Effective Date, and will terminate when all PHI provided by Member to Alliance, or created or received by Alliance on behalf of Member, is destroyed or returned to Member. If it is infeasible to return or destroy PHI, Alliance will extend the protections to such information, in accordance with Section 5.3.

5.2 Termination for Cause. Upon Member's knowledge of a material breach by Alliance of this BAA, Member will provide written notice to Alliance detailing the nature of the breach and providing an opportunity to cure the breach within thirty (30) business days. Upon the expiration of such thirty (30) day cure period, Member may terminate this BAA and, at its election, the Underlying Agreement, if Alliance does not cure the breach or if cure is not possible. Notwithstanding the above, Alliance agrees that if Member determines that Alliance has violated a material term of this BAA or HIPAA, Member has the option to either immediately terminate the Underlying Agreement and this BAA.

5.3 Effect of Termination.

5.3.1 Except as provided in Section 5.3.2, upon termination of the Underlying Agreement or this BAA for any reason, Alliance will return or destroy all PHI received from Member, or created or received by Alliance on behalf of Member, and will retain no copies of the PHI. This provision will apply to PHI that is in the possession of subcontractors or agents of Alliance.

5.3.2 If it is infeasible for Alliance to return or destroy the PHI upon termination of the Underlying Agreement or this BAA, Alliance will: (a) extend the protections of this BAA to such PHI and (b) limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Alliance maintains such PHI.

SECTION 6: COOPERATION IN INVESTIGATIONS

The parties acknowledge that certain breaches or violations of this BAA may result in litigation or investigations pursued by federal or state governmental authorities of the United States resulting in civil liability or criminal penalties. Each Party will cooperate in good faith in all respects with the other Party in connection with any request by a federal or state governmental authority for additional information and documents or any governmental investigation, complaint, action or other inquiry.

SECTION 7: SURVIVAL

The respective rights and obligations of Alliance under this BAA will survive the termination of this BAA and the Underlying Agreement.

SECTION 8: EFFECT OF BAA

In the event of any inconsistency between the provisions of this BAA and the Underlying Agreement, the provisions of this BAA will control. In the event of inconsistency between the provisions of this BAA and mandatory provisions of the Privacy Rule, the Security Rule or the HIPAA Final Rule, or their interpretation by any court or regulatory agency with authority over Alliance or Member, such interpretation will control; provided, however, that if any relevant provision of the Privacy Rule, the Security Rule or the HIPAA Final Rule is amended in a manner that changes the obligations of Alliance or Member that are embodied in terms of this BAA, then the Parties agree to negotiate in good faith appropriate non-financial terms or amendments to this BAA to give effect to such revised obligations. Where provisions of this BAA are different from those mandated in the Privacy Rule, the Security Rule, or the HIPAA Final Rule, but are nonetheless permitted by such rules as interpreted by courts or agencies, the provisions of this BAA will control.

SECTION 9: GENERAL

This BAA is governed by, and will be construed in accordance with, the laws of the State that govern the Underlying Agreement. Any action relating to this BAA must be commenced within two years after the date upon which the cause of action accrued. This BAA may only be assigned in connection with an assignment of the Underlying Agreement. If any part of a provision of this BAA is found illegal or unenforceable, it will be enforced to the maximum extent permissible, and the legality and enforceability of the remainder of that provision and all other provisions of this BAA will not be affected. All notices relating to the Parties' legal rights and remedies under this BAA will be provided in writing to a Party, will be sent to its address set forth in the Underlying Agreement, or to such other address as may be designated by that Party by notice to the sending Party, and will reference this BAA. This BAA may be modified, or any rights under it waived, only by a written agreement executed by the authorized representatives of the Parties. The Parties agree to take such action as is necessary to amend this BAA from time to time as is necessary for the Parties to comply with the requirements of applicable law. Nothing in this BAA will confer any right, remedy, or obligation upon anyone other than Member and Alliance. This BAA is the complete and exclusive agreement between the Parties with respect to the subject matter hereof, superseding and replacing all prior agreements, communications, and understandings (written and oral) regarding its subject matter. Any ambiguity in this BAA shall be resolved in favor of the meaning that permits the Parties to comply with applicable law and any current regulations promulgated thereunder. Any failure of a Party to exercise or enforce any of its rights under this BAA will not act as a waiver of such rights.