COMMONWELL HEALTH ALLIANCE®
END USER LICENSE AGREEMENT (EULA)

THIS COMMONWELL HEALTH ALLIANCE ("ALLIANCE") END USER LICENSE AGREEMENT ("EULA") SETS FORTH THE TERMS AND CONDITIONS BETWEEN ALLIANCE AND AN AUTHORIZED USER OF ITS SERVICES (TOGETHER THE "PARTIES").

BY ACCESSING OR USING THE SERVICES OR RESULTS OF THE SERVICES IN ANY WAY, INCLUDING WITHOUT LIMITATION, USING ALLIANCE NETWORKS, DATA OR OTHERWISE PARTICIPATING IN THE SERVICES, YOU AGREE TO BE BOUND BY THIS EULA. IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, YOU MAY NOT ACCESS OR USE THE SERVICES. IF YOU ARE ENTERING INTO THIS EULA ON BEHALF OF A CORPORATION OR OTHER ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO AGREE TO THE EULA ON BEHALF OF SUCH ENTITY AND THAT SUCH ENTITY AND ITS AFFILIATES ALSO AGREE TO AND ARE BOUND BY THE EULA. IF YOU DO NOT HAVE SUCH AUTHORITY, OR SUCH ENTITY DOES NOT AGREE WITH THESE TERMS, YOU AND THEY MAY NOT USE THE SERVICES.

The term "Authorized User" means a party that accesses or uses the Services in accordance with an authorized Use Case that has agreed to this EULA either directly or by reference with a party authorized by Alliance or an Authorized User to use this EULA as set forth in Section 2.1. Capitalized terms not otherwise defined in tis EULA are defined in Section 8 of this EULA.

Authorized User understands and agrees that this EULA is a legally binding agreement between such party and the Alliance, and that Service Provider is a third-party beneficiary of the EULA.

1 Introduction

The Alliance has been established to define and promote a national infrastructure with common standards and policies with regard to its Services that enable trusted data sharing among its Members who participate in the Services, their Authorized Users, and Affiliated Networks on a nation-wide basis. In order to further the foregoing mission, Alliance has procured certain services, through its Service Provider, which is made available to Authorized Users under the terms and conditions of this EULA and terms incorporated herein by reference. Therefore, for good and valuable consideration the sufficiency of which the Parties confirm, the Parties hereby agree to the above and the following terms and conditions.

2 Required Minimum Terms

2.1 Minimum Terms. If Authorized User is not an End User, Authorized User shall ensure that this EULA is incorporated in its entirety, either directly or by reference, into a legally binding agreement ("Downstream Agreement(s)") between Authorized User and any subsequent downstream authorized user (each a "Downstream Authorized User") before such Downstream Authorized User is allowed access to or provides access to the Services. For the purpose of this EULA the term "End User" means the last person or party in the chain of Authorized Users/Downstream Authorized Users in an authorized Use Case, which may be a Provider, Individual User, or other final consumer of the Services in accordance with an approved Use Case.

2.2 Application of this EULA. Each Authorized User and each Downstream Authorized User that receives this EULA from an upstream Authorised User shall be deemed the Authorized User as such term is used in this EULA and shall comply with the obligations applicable to Authorized User in this EULA.

3 Authorized User Obligations

3.1 Health Data. Authorized User understands and agrees that the Services may involve the exchange of Health Data of Authorized User, and each Licensed User, and others that may submit Health Data

involved in an approved Use Case, and that such Health Data may be used and disclosed by Alliance solely for the operation of the Services.

3.2 Authority and Consent. Authorized User represents and warrants that: (a) it has all rights and authority necessary to agree to and comply with the use of Health Data as provided in this EULA and applicable Use Cases, (b) all Health Data provided to Alliance and Service Provider or exchanged through the Services by Authorized Users and its Licensed Users is provided with the full authority and consent of the owner of such Health Data, and (c) Authorized Users shall use or disclose data received from other participants in the Services only in accordance with Applicable Laws, including but not limited to obtaining any and all required consents, and only in accordance with an authorized Use Case.

3.3 Informed Consent. Authorized User shall provide, or ensure that reasonable and required training is provided, to End Users regarding the use of the Services in accordance with the terms and conditions of this EULA, Alliance Policies, Applicable Law, and any applicable Documentation. Authorized User shall ensure that any and all required Patient and Individual User consents are obtained, and: (a) made with full transparency and education; (b) adequate to allow for all Services approved by the Alliance; (c) made only after the patient has had sufficient time to review educational material; (d) commensurate with circumstances for why health information is exchanged; (e) not used for discriminatory purposes or as a condition for receiving medical treatment; (f) consistent with patient expectations; (g) revocable at any time, and (h) recorded in a manner that allows confirmation of the name of the person and the consent.

3.4 Limitations of Use. Authorized User understands and agrees that unless expressly authorized in Section 4 (Permissions and Limitations) of this EULA the following are prohibited: (a) marketing, selling, licensing or distributing the Services; (b) licensing or sub-license the Services to any person or entity; (c) renting, leasing, providing access to, or granting a security interest in, or otherwise transferring or attempting to transfer any rights in or to the Services; (d) removing, altering, defacing any legends, restrictions, product identifications, or copyright, trademark or other proprietary notices from the Services or the Alliance Specification, or; (e) reverse engineering or otherwise deriving the source code or the reasonable equivalent of the Services or any software related thereto or therein. For the purpose of this Section, the Services includes all Service Provider and Alliance materials, software, technologies and documentation related to the Services.

3.5 Compliance with Applicable Laws and Alliance Policies. Authorized User shall: (a) use the Services only in accordance with the terms and conditions of this EULA; and (b) 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.

3.6 Compliance with Alliance Policies. Authorized User represents and warrants that it will, and shall require its Downstream Authorized Users to, comply with all applicable Alliance Policies, available here: www.commonwellalliance.org/policies, where such policies may be updated from time to time.

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

3.8 Account Management. Authorized User, when it access the Services via a log-in portal, shall require each person accessing the Services, through such logon features, to enter his or her login credentials ("Login Credentials") in order to access the Services. Authorized Users shall obligate Permitted Users who access the Services through log in portals to comply with this Section. Authorized User is fully responsible for all uses of Login Credentials issued to or created for or by Authorized User. Authorized User is responsible for authentication and identity management of each person that accesses the Services and to ensure such Login Credentials are unique to each person and that such information remains secure. Authorized User shall ensure that each person accessing clinical data using the Services is properly identified, authenticated and authorized under Applicable Laws to access such Health Data.

3.9 Breach Detection and Notification. Authorized User shall comply with all applicable breach notification requirements pursuant to 45 CFR § 164.410. Authorized User shall make reasonable efforts to notify Alliance of any Breach of Confidentiality or Security within three (3) days from discovery, and shall report any Breach in accordance with the Alliance Breach Incident Notification Policy available here https://www.commonwellalliance.org/policies/.

3.10 Data Backup. Authorized User is responsible for providing or operating data back-up services, and other procedures and controls appropriate to maintain the integrity and continuity of their operations, including the protection of their data and PHI or of their End Users.

3.11 External Transaction Services Terms. The Services may include products and services available to Authorized User that involve access to, use of, and re-disclosure of information allowed by Alliance, but governed by third parties ("External Transaction Services"). If Authorized User has access to or uses External Transaction Services, Authorized User understands and agrees that they shall comply with the terms and conditions applicable to such services, as updated from time to time, and which are available here https://www.commonwellalliance.org/policies/.

3.12 ROI Services. If Authorized User participates in ROI Services as a Data Retrieval Vendor, Authorized User represents and warrants that it shall comply with the following terms ("ROI Connection Terms"):

3.12.1 When required for a Use Case, Authorized User shall be certified pursuant to a mutually approved ROI Certification Process prior to participation (such certified Authorized User to be referred to as "ROI Members"), and;

3.12.2 if Authorized User is a Data Retrieval Vendor, Record Copier or EHR Vendor, Authorized User represents and warrants that it: (i) has obtained and stored all necessary directives, consents and authorizations required under applicable law and regulations for use and disclosure of PHI in accordance with ROI Use Cases, and (ii) shall not direct the use and disclosure of PHI except as permitted by the ROI Use Case.

3.12.3 Authorized Users providing ROI Services to Downstream Authorized Users represent and warrant that they shall include the ROI Connection Terms, and the following in its Downstream Agreements:

3.12.3.1 The ROI Connection Terms constitute a binding written agreement between such ROI Member and Alliance;

Service Provider and Alliance shall be third-party beneficiaries of the payment terms between Authorized User and Data Retrieval Vendors and the Data Requestors.

3.13 Connectors. If Authorized User will be operating as a Connector, Authorized User represents and warrants that it shall comply with the following terms ("Connector Terms"):

3.13.1 When required for a Use Case, Authorized User will be certified pursuant to a mutually approved Connector Certification Process for the applicable Use Case prior to participation (such certified Authorized User to be referred to as "Connector"), and;

3.13.2 Authorized User represents and warrants that it: (i) has obtained and stored all necessary directives, consents and authorizations required under applicable law and regulations for use and disclosure of PHI in accordance with a Connector Use Case, and (ii) shall not direct the use and disclosure of PHI except as permitted by the Connector Use Case.

3.13.3 Authorized User represents and warrants that it shall inform Alliance of its connections on a

monthly basis, using an approved report format, such report to include a directory all applicable Downstream Authorized Users.

4 Permissions and Limitations

4.1 License to Authorized User. Conditioned upon compliance with the terms and conditions of this EULA, Authorized User is hereby granted a limited, nonexclusive, non-transferable, non-sublicensable license to access the Services, only for purposes approved by the Alliance in an approved Use Case, and to allow access to the Services by Licensed Users in accordance with an approved Use Case.

4.2 License to Licensed Users. Conditioned upon compliance with the terms and conditions of this EULA, Licensed User is hereby granted a limited, nonexclusive, non-transferable, non-sublicensable, license, to access and use the Services, only for purposes approved by the Alliance in an approved Use Case, and only for its own internal or individual use.

4.3 Alliance License to use Data and PHI. Authorized User(s) grants Alliance the right to use data, including but not limited to Data, PHI and de-identified PHI acquired through the Services: (a) solely to provide the Services for the benefit of the Alliance and its Members; (b) to improve the Services, and; (c) for system administration of the Services, and for no other purposes. Notwithstanding the foregoing, nothing herein shall be deemed to restrict Alliance from using Data and PHI to create de-identified data which may be used to improve or enhance the Services, and to provide the Services in accordance with approved Use Cases. Alliance 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 related to approved Use Cases. For the avoidance of doubt, any reference to Alliance in Section 4 shall mean Alliance and its Service Provider(s).

4.4 Alliance Data Use Limitations. Without limitation, except as permitted by this Section 4 or otherwise permitted by the EULA, Alliance shall not modify, transform, conduct analysis on, or otherwise use Data and PHI in any manner except as necessary to provide the Services.

4.5 Limited License to Alliance Marks. Subject to the terms and conditions of this EULA, Alliance grants Authorized User 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 Services and otherwise as necessary or appropriate for Authorized User to exercise its rights or perform its obligations under this EULA, all subject to Authorized User's compliance with the Alliance's Trademark Usage Guidelines, available here https://www.commonwellalliance.org/policies/, as may be modified from time to time. Authorized User 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 Authorized User's use of the Alliance Marks inure solely to the benefit of Alliance. All use of Alliance Marks are at the sole discretion of the Alliance, and Alliance has the sole and exclusive right to deny the use of Alliance Marks by any party.

4.6 Limited License to Authorized User Marks. Subject to the terms and conditions of this EULA, Authorized User grants Alliance a non-exclusive, non-transferable right to use and display the Authorized User trademarks and service marks provided by Authorized User, as may be updated from time to time in Authorized User's sole discretion (the "Authorized User 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 EULA. Alliance acknowledges and agrees that Authorized User owns the Authorized User Marks and that any and all goodwill and other proprietary rights that are created by or that result from Alliance's use of the Authorized User Marks inure solely to the benefit of Authorized User.

4.7 Retention of Rights and Termination of License. The Services are licensed and not sold. Except for the rights specifically granted in Section 4, Service Provider, Alliance, and their licensors retain all rights title and interest in and to their Intellectual Property, and there are no implied licenses thereto, whether implied, statutory, or otherwise. The Services and all additions or modifications to the Services,

including derivative works thereof, all Intellectual Property rights associated therewith, are the sole and exclusive property of Alliance and Service Provider, or their licensors. Any license granted in Section 4 of this EULA shall automatically lapse in the event of a breach or any of the terms and conditions of this EULA, including but not limited to a breach of Section 3.4 (Limitations of Use).

5 Suspension of Services

Alliance and Service Provider each retain the right to suspend or terminate the Services provided to Authorized User or any Licensed User at any time in the event that Authorized User or Licensed User is not in material compliance with this EULA, or where such suspension is determined at the sole discretion of Alliance to be in the best interest of the Alliance, its Members, Authorized Users, or to protect the performance, integrity or security of the Services.

6 Disclaimers and Limitations of Liability

6.1 Alliance disclaims all representations and warranties with regards to the accuracy and or completeness of any Health Data provided or accessed through the Services.

6.2 Health Data, including content, disclosed or received through the Services may not be a complete clinical record or history with respect to any individual, and any such data or content is not a substitute for a healthcare provider's professional judgement for or in the proper treatment of a patient. It is the responsibility of any treating Provider to confirm the accuracy and completeness of any Health Data or clinical records used for treatment purposes and it is the responsibility of the Provider to obtain whatever information the provider deems necessary, in his/her professional judgment, for the proper treatment of a patient.

6.3 Providers are 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 Alliance assumes no responsibility or role in the care of any patient.

6.4 **Notice to Individual Users. If the End User is an Individual, all data and Health Data is provided to such individual on an as-is, as available basis, with no warranty of any kind, and for information purposes only. Neither the Services nor any Data or Health Data provided in or through the Services shall be deemed medical advice.**

6.5 LIMITATION OF LIABILITY. IN NO EVENT WILL ALLIANCE OR SERVICE PROVIDER BE LIABLE TO AUTHORIZED USER, LICENSED USERS, INDIVIDUALS, OR ANY OTHER PARTY, UNDER, IN CONNECTION WITH, OR RELATED TO THE EULA OR THE SERVICES, INCLUDING FOR ANY SPECIAL, INCIDENTAL, INDIRECT, OR CONSEQUENTIAL DAMAGES OF ANY KIND, INCLUDING, BUT NOT LIMITED TO, LOST PROFITS OR LOSS OF GOODWILL, LOST DATA, 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 AGGREGATE, CUMULATIVE LIABILITY FOR ANY AND ALL LOSS OR DAMAGE, DIRECT OR INDIRECT, FOR ANY CAUSE WHATSOEVER AND REGARDLESS OF THE FORM OF ACTION, RELATED TO THE EULA AND THE SERVICES, OR USE THEREOF, SHALL BE LIMITED TO $5,000.

6.6 THE ALLIANCE AND SERVICE PROVIDER CANNOT REVIEW OR CONFIRM THE ACCURACY OF DATA OR HEALTH DATA OR PHI THAT IS USED IN OR THROUGH THE SERVICES. THEREFORE, THE SERVICES AND ANY DATA OR HEALTH DATA IN OR ACCESSED THROUGH THE SERVICES ARE PROVIDED ON AN "AS-IS" AND "AS-AVAILABLE" BASIS. ALLIANCE AND SERVICES PROVIDER EXPRESSLY DISCLAIM ALL WARRANTIES OF ANY KIND, WHATSOEVER, WHETHER EXPRESS OR IMPLIED, OR OTHERWISE, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR

A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF INTELLECTUAL PROPERTY WITH RESPECT TO THE SERVICES, INCLUDING THE RESULTS OF THE SERVICES.

ALLIANCE AND SERVICES PROVIDER MAKE NO WARRANTIES AND DISCLAIM ALL WARRANTIES THAT: (A) THE SERVICES WILL BE AVAILABLE ON AN UNINTERRUPTED, TIMELY, SECURE, OR ERROR-FREE BASIS; (B) ANY RESULTS OBTAINED FROM THE USE OF THE SERVICES WILL BE ACCURATE OR RELIABLE; (C) THE SERVICES WILL MEET A USER'S REQUIREMENTS. ANY DATA OR PHI ACCESSED OR OTHERWISE OBTAINED ON OR THROUGH THE USE OF THE SERVICES ARE AT AUTHORIZED USER'S AND OTHER USERS' OWN DISCRETION AND RISK. ALLIANCE RESERVES THE RIGHT TO MODIFY OR DISCONTINUE THE SERVICES WITHOUT NOTICE AND SHALL NOT BE LIABLE FOR ANY LOSS OR DAMAGES RESULTING THEREFROM.

7 *General Terms*

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

7.2 Export Control. This EULA is subject to governmental laws, orders and other restrictions regarding the export, import, re-export or use ("Control Laws") of the Services and Documentation, including technical data and related information ("Regulated Materials"). Authorized User shall 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.

7.3 Insurance. Authorized User agrees, at its own expense, to maintain commercially reasonable insurance, including as required by Applicable Law, and which may include where applicable, self-insurance.

7.4 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 EULA 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.

7.5 Governing Law and Venue. This EULA 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. Any legal action or proceeding arising under this Agreement will be brought exclusively within the state of Delaware, and the Parties hereby consent to personal jurisdiction and venue therein.

7.6 Assignment. Authorized User may not transfer, assign, sublicense or otherwise delegate any of its rights or obligations under this EULA, by operation of law or otherwise.

7.7 Severability. If any part of a provision of this EULA 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 EULA will not be affected.

7.8 Construction of Agreement. This EULA will not be presumptively construed for or against any Party.

7.9 Order of Precedence. In the event of any conflict or inconsistency between or among Applicable Law, this EULA, Downstream Agreements, and Alliance Policies, the following shall be the order of precedence to the extent of such conflict or inconsistency: (i) Applicable Law, (ii) this EULA, (iii) Alliance Policies, (iv) applicable Downstream Authorized User Agreement, then (v) any other terms and conditions.

7.10 Entire Agreement. This EULA, including the Policies 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.

8 Definitions

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

"Affiliated Networks" means networks that operate with or connect to the Alliance Services and/or network, including those currently existing and those that may come to exist in the future.

"Alliance Policies" means all policies approved by the Alliance relating to the Alliance or the Services, as updated from time to time.

"Alliance Specification" means each document designated a "CommonWell Health Alliance Specification" as finally adopted and approved by the Alliance. The most current version of the Alliance Specification may be obtained here: https://www.commonwellalliance.org/connect-to-the-network/use-cases-and-specifications/

"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 applicable foreign country or any domestic or foreign state, county, city or other political subdivision, including without limitation agreements and operating procedures required to operate with any government agency or government sponsored healthcare exchange.

"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 compromises the security or privacy of information of Alliance, Service Provider, or any Member.

"Connector" means a Member that contracts directly with an EHR Vendor in a manner that allows the EHR Vendor to allow its customers access to the Services.

"Data" means the information and files that an Authorized User may receive from or deliver to Alliance, a Service Provider, through the Services, but not PHI.

"Data Requestors" means the entities requesting clinical data pursuant to approved ROI Use Cases.

"Data Retrieval Vendor" means the ROI Members who contract with Data Requestors to fulfil health record requests through the ROI 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.

"Downstream Authorized User" means a party with a written agreement directly with an Authorized User requiring compliance with this EULA, and each subsequent Downstream Authorized User.

“EHR Vendor” or “EHR” means an electronic health records provider, or as it relates to ROI Services, it means an ROI Member that provides the Alliance with access to a patient record.

“End User” means the last person or party in the chain of Authorized Users in an authorized Use Case, which may be a Provider, Individual User, or other final consumer of the Services in accordance with an approved Use Case.

“Health Data” means information, health 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.

“Individual User” means an individual that uses the Services on an individual basis, and where such individual is not an End User or Patient, such as a PHR user or Licensed User.

“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.

“Licensed User(s)” means a third party authorized by an Authorized User to accesses or use the Services in accordance with an authorized Alliance Use Case.

“Member” means legal entity that is a party to a valid Alliance Membership Agreement with Alliance.

“Patient” means an individual that has access to or is a recipient of the Services through or on behalf of a Provider.

“Permitted User(s)” means users permitted by Authorized User to access or use the Services on behalf of Authorized User or its Licensed Users, including Authorized User personnel who access the Services through Login Credentials in order to access the Services. Authorized User are responsible for their Permitted Users compliance with this EULA.

“Personal Health Record” or “PHR” means is an electronic application through which Patients can access, maintain and/or manage their health information.

“Provider” means a healthcare provider facility, practice group, physician (including any individual or legal entity), or other health care provider permitted by a Authorized User to access the Services or any enrollment user interface to utilize the Services.

“Protected Health Information” or “PHI” means 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 on behalf of its Members. All references to PHI include Electronic PHI.

“ROI Certification Process” means the process by which new ROI Members certify compliance with the ROI Services Connection Terms. Service Provider shall be responsible for certification, onboarding, and setup support for ROI Members.

“ROI Services” means services related to requests for patient data in accordance with an approve Use Case, for example fulfillment of payer requests for patient data.

“Services” means the services approved and offered by or on behalf of the Alliance in accordance with an approved Use Case. Services may also include offerings from Affiliated Networks.

“Service Provider” means a party that Alliance has contracted with to provide the Services (or a subset of the Services).

“Use Case” means a use case approved by the Alliance, as further defined in the Alliance Specification, including a list of technical specifications, obligations, and events, necessary to implement a compliant implementation of such use case.

CommonWell Health Alliance
External Transaction Services Terms and Conditions

The following terms and conditions, including any additional terms and conditions incorporated by reference ("Additional Terms"), shall apply to your access or use of the below described External Transaction Services.

The defined terms in this Schedule, not otherwise defined herein, shall have the meanings provided in the MSA, or in applicable Additional Terms.

Authorized Users shall be responsible for any applicable fees associated with External Transaction Services.

Carequality Services

1. Carequality Services. In the event Authorized User uses Services that involve access to, use of, and re-disclosure of information that the Alliance obtains by virtue of being a Carequality Implementer (the "Carequality Services"), Authorized User shall comply with these additional terms and conditions.

2. Carequality Obligations. Prior to accessing or using Carequality Services, Authorized User represents and warrants that it: (a) shall comply with all applicable Carequality Connection Terms or other applicable terms and conditions for adopted Carequality Use Cases; (b) understands that the Carequality Connection Terms constitute a binding written agreement between Authorized User and Alliance, and; (c) it has received adequate authority and consents from Authorized User to participate in the Carequality Services, including but not limited to any applicable exchange Activity related thereto. For the purpose of this agreement "Carequality Connection Terms" means the Carequality terms and conditions, which may be updated from time to time and available from Carequality, available here: [https://carequality.org/resources/]. For the purpose of this Agreement "Carequality Implementer" has the meaning provided in the Carequality Connection Terms.

3. Carequality Services and Fees. Authorized User electing to use or access Carequality Services shall be obligated to pay any applicable Carequality fees.

4. Alliance and Authorized User Obligations. Alliance and Authorized User 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 Authorized User and Alliance with respect to the Carequality Services, which shall be deemed 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 Member and participants.

TEFCA Services

If Authorized User desires to participate in the transmission of information for one or more of the Exchange Purposes and related activities under TEFCA through the Alliance in its capacity as a QHIN ("QHIN Services"), Alliance is required flow down to Authorized User certain Required Flow-Downs to ensure that Alliance legally binds Authorized User to certain specific terms and conditions of the Common Agreement.

1. Prior to accessing or using TEFCA Services, Authorized User represents and warrants that it: (a) shall comply with all applicable terms and conditions of the Required Flow-Downs, available here www.commonwellalliance.org/policies.

2. In addition to the Required Flow Down Terms, there are other sections of the Common Agreement that apply to Authorized User (e.g., notification of TEFCA Security Incidents).

3. The Required Flow-Down provisions apply only to transmission of information for one or more of the Exchange Purposes and related activities.

4. No Exclusivity. Section 6.2.1 of the Common Agreement prohibits exclusivity, so the terms in this document are not required to apply to the exchange of information with, conducting other transactions with, or supporting any other networks or exchange frameworks using services other than the QHIN Technical Framework involving QHIN--to-QHIN exchange as one step in the transmission.

CommonWell Health Alliance, Inc.
TEFCA
Required Flow-Down(s)

[Version: 05 December 2023]

Subject to change upon update to TEFCA Common Agreement

1. **Defined Terms.** Capitalized terms used in this Amendment shall have the meaning set forth below for purposes of the activities contemplated herein. Where a definition includes one or more citations to a statute, regulation, or standard, the definition shall be interpreted to refer to such statute, regulation, or standard as may be amended from time-to-time.

   Applicable Law: all federal, state, local, or tribal laws and regulations then in effect and applicable to the subject matter herein. For the avoidance of doubt, federal agencies are only subject to federal law.

   Business Associate: has the meaning assigned to such term at 45 CFR § 160.103.

   Business Associate Agreement (BAA): a contract, agreement, or other arrangement that satisfies the implementation specifications described within 45 CFR § 164.504I, as applicable.

   Common Agreement: unless otherwise expressly indicated, the *Common Agreement for Nationwide Health Information Interoperability* that has been entered into by and between Alliance and the RCE, including as may be amended, along with the QHIN Technical Framework (QTF), all Standard Operating Procedures (SOPs), and all other attachments, exhibits, and artifacts incorporated therein by reference.

   Confidential Information: Any information that is designated as Confidential Information by the person or entity that discloses it (a "Discloser"), or that a reasonable person would understand to be of a confidential nature, and is disclosed to another person or entity (a "Recipient") pursuant to this Amendment. For the avoidance of doubt, "Confidential Information" does not include electronic protected health information (ePHI), as defined in this Participant-QHIN Agreement, that is subject to a Business Associate Agreement and/or other provisions of this Amendment.

   Notwithstanding any label to the contrary, "Confidential Information" does not include any information that: (i) is or becomes known publicly through no fault of the Recipient; or (ii) is learned by the Recipient from a third party that the Recipient reasonably believes is entitled to disclose it without restriction; or (iii) is already known to the Recipient before receipt from the Discloser, as shown by the Recipient's written records; or (iv) is independently developed by Recipient without the use of or reference to the Discloser's Confidential Information, as shown by the Recipient's written records, and was not subject to confidentiality restrictions prior to receipt of such information

from the Discloser; or (v) must be disclosed under operation of law, provided that, to the extent permitted by Applicable Law, the Recipient gives the Discloser reasonable notice to allow the Discloser to object to such redisclosure, and such redisclosure is made to the minimum extent necessary to comply with Applicable Law.

Connectivity Services: the technical services provided by a QHIN consistent with the requirements of the then-applicable QHIN Technical Framework and pursuant to the Common Agreement and provided by Alliance to Participant consistent with the Required Flow-Downs with respect to all Exchange Purposes.

Covered Entity: has the meaning assigned to such term at 45 CFR § 160.103.

Designation (including its correlative meanings "Designate," "Designated," and "Designating"): the RCE's written confirmation to ONC that a HIN has satisfied all the requirements of the Common Agreement, the QHIN Technical Framework, and all applicable SOPs and is now a QHIN.

Direct Relationship: a relationship between (1) an Individual and (2) a QHIN, Participant, or Subparticipant, that arises when the QHIN, Participant, or Subparticipant, as applicable, offers services to the Individual in connection with one or more of the Framework Agreements, and the Individual agrees to receive such services.

Disclosure (including its correlative meanings "Disclose," "Disclosed," and "Disclosing"): the release, transfer, provision of access to, or divulging in any manner of TI outside the entity holding the information.

Discovery: for purposes of determining the date on which a TEFCA Security Incident was discovered, the term Discovery shall be determined consistent with 45 CFR § 164.404(a)(2) as if the TEFCA Security Incident were a breach (as defined in 45 CFR § 164.402) except that this term shall also apply to Non-HIPAA Entities.

Dispute: means (i) a disagreement about any provision of this Common Agreement, including any SOP, the QTF, and all other attachments, exhibits, and artifacts incorporated by reference; or (ii) a concern or complaint about the actions, or any failure to act, of Signatory, the RCE, or any other QHIN or another QHIN's Participant(s).

Dispute Resolution Process: the non-binding dispute resolution process set forth in the *Dispute Resolution Process SOP*.

Downstream Subparticipant: a Subparticipant that has entered into a Downstream Subparticipant Agreement to use the services of another Subparticipant (referred to as the "Upstream Subparticipant") to send and/or receive information as described in Section 9 of the Common Agreement.

Downstream Subparticipant Agreement: an agreement that incorporates all of the

Required Flow-Downs of the Common Agreement and is between a Subparticipant (referred to as the "Upstream Subparticipant") and one or more Subparticipants (each a "Downstream Subparticipant"), which enables the Downstream Subparticipant(s) to use the services of the Upstream Subparticipant as described in Section 9 of the Common Agreement to send and/or receive information for one or more Exchange Purposes; provided, however, that any provisions of said agreement that permit or require activities other than those required or permitted by the Common Agreement shall not be deemed part of the Downstream Subparticipant Agreement as defined herein. For example, if the agreement provides for transmission of information for reasons other than the Exchange Purposes, the provisions governing such activities shall not be deemed part of the Downstream Subparticipant Agreement as defined herein. Any Subparticipant may enter into a Downstream Subparticipant Agreement.

Electronic Protected Health Information (ePHI): has the meaning assigned to such term at 45 CFR § 160.103.

Exchange Purpose(s): means the reason, as authorized by the Common Agreement, including the Exchange Purposes SOP, for a Request, Use, Disclosure, or Response transmitted via QHIN-to-QHIN exchange as one step in the transmission. Authorized Exchange Purposes are: Treatment, Payment, Health Care Operations, Public Health, Government Benefits Determination, Individual Access Services, and any other purpose authorized as an Exchange Purpose by the Exchange Purposes SOP, each to the extent permitted under Applicable Law, under all applicable Required Flow-Down provisions of the Common Agreement, and, if applicable, under the implementation SOP for the applicable Exchange Purpose.

Framework Agreement(s): any one or combination of the Common Agreement, a Participant-QHIN Agreement, a Participant-Subparticipant Agreement, or a Downstream Subparticipant Agreement, as applicable.

Government Benefits Determination: a determination made by any federal, state, local, or tribal agency, instrumentality, or other unit of government as to whether an Individual qualifies for government benefits for any purpose other than health care (for example, Social Security disability benefits) to the extent permitted by Applicable Law. Disclosure of TI for this purpose may require an authorization that complies with Applicable Law.

Government Health Care Entity: any agency, instrumentality, or other unit of the federal, state, local, or tribal government to the extent that it provides health care services (e.g., Treatment) to Individuals but only to the extent that it is not acting as a Covered Entity.

Health Care Operations: has the meaning assigned to such term at 45 CFR § 164.501, except that this term shall apply to the applicable activities of a Health Care Provider regardless of whether the Health Care Provider is a Covered Entity.

Health Care Provider: has the meaning assigned to such term in the information

blocking regulations at 45 CFR § 171.102 or in the HIPAA Rules at 45 CFR § 160.103.

Health Information Network (HIN): has the meaning assigned to the term "Health Information Network or Health Information Exchange" in the information blocking regulations at 45 CFR § 171.102.

HIPAA: the Health Insurance Portability and Accountability Act of 1996 codified at 42 U.S.C. § 300gg, 29 U.S.C. § 1181 *et seq.,* 42 U.S.C. § 1320d *et seq*., and the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 codified at 42 U.S.C. § 17921 et seq., and 42 U.S.C. § 17931 et seq.

HIPAA Rules: the regulations set forth at 45 CFR Parts 160, 162, and 164.

HIPAA Privacy Rule: the regulations set forth at 45 CFR Parts 160 and 164, Subparts A and E.

HIPAA Security Rule: the regulations set forth at 45 CFR Part 160 and Part 164, Subpart C.

Individual: one or more of the following:

(1) An individual as defined by 45 CFR 160.103;

(2) Any other natural person who is the subject of the information being Requested, Used, or Disclosed;

(3) A person who legally acts on behalf of a person described in paragraphs (1) or (2) of this definition in making decisions related to health care as a personal representative, in accordance with 45 CFR 164.502(g);

(4) A person who is a legal representative of and can make health care decisions on behalf of any person described in paragraphs (1) or (2) of this definition; or

(5) An executor, administrator, or other person having authority to act on behalf of a deceased person described in paragraphs (1) or (2) of this section or the individual's estate under Applicable Law.

IAS Provider: Each QHIN, Participant, and Subparticipant that offers Individual Access Services.

Individual Access Services (IAS): with respect to the Exchange Purposes definition, the services provided utilizing the Connectivity Services, to the extent consistent with Applicable Law, to an Individual with whom the QHIN, Participant, or Subparticipant has a Direct Relationship to satisfy that Individual's ability to access, inspect, or obtain a copy of that Individual's Required Information that is then maintained by or for any QHIN, Participant, or Subparticipant.

Individually Identifiable: refers to information that identifies an Individual or with respect to which there is a reasonable basis to believe that the information could be

used to identify an Individual.

Minimum Necessary: refers to the provision in the HIPAA Rules that, under certain circumstances, requires a Covered Entity or a Business Associate to make reasonable efforts when Using or Disclosing PHI or when Requesting PHI from another Covered Entity or Business Associate to limit PHI to the minimum necessary to accomplish the intended purpose of the Use, Disclosure, or Request. See 45 CFR §164.502(b) and §164.514(d).

Non-HIPAA Entity (NHE): a QHIN, Participant, or Subparticipant that is neither a Covered Entity nor a Business Associate under HIPAA with regard to activities under the applicable Framework Agreement.

Onboarding: the process Signatory, a Participant, or a Subparticipant must undergo to become a QHIN, Participant, or Subparticipant and operational in the production environment under the Framework Agreement to which it is a party. For Signatory, the Onboarding requirements shall be set forth in the Onboarding & Designation SOP addressing the process toward Designation as a QHIN. For a Participant, the Onboarding requirements shall be set forth in the Participant-QHIN Agreement. For a Subparticipant, the Onboarding requirements shall be set forth in the Subparticipant Agreement or the Downstream Subparticipant Agreement, as applicable.

ONC: the U.S. Department of Health and Human Services Office of the National Coordinator for Health Information Technology.

Organized Health Care Arrangement: has the meaning assigned to such term at 45 CFR § 160.103.

Participant: to the extent permitted by applicable SOP(s), a U.S. Entity regardless of whether the entity is a Covered Entity or a Business Associate, that has entered into a Participant-QHIN Agreement whereby the QHIN agrees to transmit and receive information via QHIN-to-QHIN exchange on behalf of the party to the Participant- QHIN Agreement for the Exchange Purposes. The Party entering into this Amendment with Alliance is a Participant.

Participant-QHIN Agreement:

An agreement that incorporates all of the Required Flow-Downs of the Common Agreement and is between a QHIN and one or more Participants; provided, however, that any provisions of said agreement that permit or require activities other than those required or permitted by the Common Agreement shall not be deemed part of the Participant-QHIN Agreement as defined herein. For example, if the agreement provides for transmission of information for reasons other than the Exchange Purposes, the provisions governing such activities shall not be deemed part of the Participant-QHIN Agreement as defined herein.

In the event of any conflict or inconsistency between or among Applicable Law, the Participant-QHIN Agreement, and any other terms and conditions, the following shall

be the order of precedence to the extent of such conflict or inconsistency: (i) Applicable Law; (ii) the provisions of the Participant- QHIN Agreement that are Required Flow-Downs under the Common Agreement; (iii) to the extent applicable, the QTF; (iv) to the extent applicable, the SOPs; and
(v) any other terms and conditions agreed to by the parties.

Participant-Subparticipant Agreement:

An agreement that incorporates all of the Required Flow-Downs of the Common Agreement and is between a Participant and one or more Subparticipants, which enables the Subparticipant(s) to use the services of the Participant as described in Section 9 of the Common Agreement to send and/or receive information for one or more Exchange Purposes; provided, however, that any provisions of said agreement that permit or require activities other than those required or permitted by the Common Agreement shall not be deemed part of the Participant-Subparticipant Agreement as defined herein. For example, if the agreement provides for transmission of information for reasons other than the Exchange Purposes, the provisions governing such activities shall not be deemed part of the Participant-Subparticipant Agreement as defined herein.

In the event of any conflict or inconsistency between or among Applicable Law, the Participant-Subparticipant Agreement, and any other terms and conditions, the following shall be the order of precedence to the extent of such conflict or inconsistency: (i) Applicable Law; (ii) the provisions of the Participant-Subparticipant Agreement that are Required Flow-Downs under the Common Agreement; (iii) to the extent applicable, the QTF; (iv) to the extent applicable, the SOPs; and (v) any other terms and conditions agreed to by the parties.

Payment: has the meaning assigned to such term at 45 CFR § 164.501.

Privacy and Security Notice: the written privacy and security notice described in Section 6.3 of this Amendment.

Protected Health Information (PHI): has the meaning assigned to such term at 45 CFR § 160.103.

Public Health: with respect to the definition of Exchange Purposes, a Request, Use, Disclosure, or Response permitted under the HIPAA Rules and other Applicable Law for public health activities and purposes involving a Public Health Authority, where such public health activities and purposes are permitted by Applicable Law, including a Use or Disclosure permitted under 45 CFR §164.512(b) and 45 CFR §164.514(e).
For the avoidance of doubt, a Public Health Authority may Request, Use, and Disclose TI hereunder for the Exchange Purpose of Public Health to the extent permitted by Applicable Law and the Framework Agreements.

Public Health Authority: has the meaning assigned to such term at 45 CFR §164.501.

QHIN Directory: has the meaning set forth in the QTF.

QHIN Technical Framework (QTF): the document described in Section 5.2 of the Common Agreement and incorporated by reference into the Common Agreement, as may be amended, that may include: (1) technical requirements, functional requirements, and privacy- and security-related requirements for the exchange of TI between QHINs; (2) internal-QHIN functional requirements; (3) technical, privacy, and security flow-down requirements from the QHIN to the Participants and/or Subparticipants (if any) in addition to the privacy and security Required Flow-Downs in the Common Agreement; and (4) operational requirements that enable the exchange of TI between and among QHINs.

Qualified Health Information Network (QHIN): to the extent permitted by applicable SOP(s), a Health Information Network that is a U.S. Entity that has been Designated by the RCE and is a party to the Common Agreement countersigned by the RCE.

RCE Directory: has the meaning set forth in the QTF.

RCE Directory Service: a technical service provided by the RCE that enables QHINs, Participants, and Subparticipants to share directory information associated with other QHINs, Participants, and Subparticipants in order to enable the exchange of TI under the Framework Agreements. The then-current technical endpoints and other identifying information of QHINs, Participants, and Subparticipants are included and maintained as part of the RCE Directory Service.

Recognized Coordinating Entity (RCE): the entity selected by ONC that enters into the Common Agreement with QHINs in order to impose, at a minimum, the requirements of the Common Agreement, including the SOPs and the QTF, on the QHINs and administer such requirements on an ongoing basis.

Request(s) (including its correlative uses/tenses "Requested" and "Requesting"): the act of asking for information in accordance with the applicable requirements of the Framework Agreements.

Required Flow-Down(s): the rights and obligations set forth within the Common Agreement that each QHIN is required to incorporate in its Participant-QHIN Agreements and that each QHIN is required to obligate its Participants to include in their Subparticipant Agreements and that QHINs must require Participants to obligate Subparticipants to impose on their Downstream Subparticipants, if any, through their Downstream Subparticipant Agreements.

Required Information:

Electronic information maintained by any QHIN, Participant, or Subparticipant prior to or during the term of the applicable Framework Agreement:

(i) that would be ePHI if maintained by a Covered Entity or a Business Associate; and

(ii) regardless of whether the information is or has already been transmitted via QHIN-to-QHIN exchange.

Notwithstanding the foregoing, the following types of information are **not** Required Information:

(a) information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; or

(b) psychotherapy notes (as defined at 45 CFR 164.501).

Response(s) (including its correlative uses/tenses "Responded" and "Responding"): the act of providing information or the information provided in accordance with the applicable requirements of the Framework Agreements.

Standard Operating Procedure(s) or **SOP(s):** a written procedure or other provision that is adopted pursuant to the Common Agreement and incorporated by reference into the Common Agreement to provide detailed information or requirements related to the exchange activities under the Common Agreement, including all amendments thereto and any new SOPs that are adopted pursuant to the Common Agreement. SOPs will be adopted to address the application process, the QHIN onboarding process, and other operational processes. Each SOP identifies the relevant group(s) to which the SOP applies, including whether Participants and/or Subparticipants are required to comply with a given SOP. An SOP shall be deemed in effect when adopted pursuant to Section 5.3 of the Common Agreement and listed on a public website.

Subparticipant: to the extent permitted by applicable SOP(s), a U.S. Entity regardless of whether the entity is a Covered Entity or Business Associate, that has entered into either: (i) a Participant-Subparticipant Agreement to use the services of a Participant as described in Section 9 of the Common Agreement to send and/or receive information; or (ii) a Downstream Subparticipant Agreement pursuant to which the services of a Subparticipant are used as described in Section 9 of the Common Agreement to send and/or receive information.

TEFCA Information (TI): any information that is exchanged between QHINs for one or more of the Exchange Purposes pursuant to any of the Framework Agreements. As a matter of general policy, once TI is received by a QHIN, Participant, or Subparticipant that is a Covered Entity or Business Associate and is incorporated into such recipient's system of records, the information is no longer TI and is governed by the HIPAA Rules and other Applicable Law.

TEFCA Security Incident(s):

(1) An unauthorized acquisition, access, Disclosure, or Use of unencrypted TI in transit using the Connectivity Services or pursuant to any Framework Agreement between a QHIN and its Participants, between Participant's and its Subparticipants, or between Subparticipants, but **NOT** including the following:

(i) Any unintentional acquisition, access, or Use of TI by a workforce member or person acting under the authority of a QHIN, Participant, or Subparticipant, if such acquisition, access, or Use was made in good faith and within the scope of authority

and does not result in further Use or Disclosure in a manner not permitted under Applicable Law and the applicable Framework Agreement.

(ii) Any inadvertent Disclosure by a person who is authorized to access TI at a QHIN, Participant, or Subparticipant to another person authorized to access TI at the same QHIN, Participant, or Subparticipant, or Organized Health Care Arrangement in which a QHIN, Participant, or Subparticipant participates or serves as a Business Associate, and the information received as a result of such Disclosure is not further Used or Disclosed in a manner not permitted under Applicable Law and the applicable Framework Agreement.

(iii) A Disclosure of TI where a QHIN, Participant, or Subparticipant has a good faith belief that an unauthorized person to whom the Disclosure was made would not reasonably have been able to retain such information.

(iv) A Disclosure of TI that has been de-identified in accordance with the standard at 45 CFR § 164.514(a).

(2) Other security events (e.g., ransomware attacks), as set forth in an SOP, that prevent the affected QHIN, Participant, or Subparticipant from responding to requests for information as required under the applicable Framework Agreement or otherwise adversely affect their participation in exchange via the Connectivity Services.

Treatment: has the meaning assigned to such term at 45 CFR § 164.501.

United States: the 50 States, the District of Columbia, and the territories and possessions of the United States including, without limitation, all military bases or other military installations, embassies, and consulates operated by the United States government.

Unsecured: has the meaning assigned to such term at 45 CFR § 164.402 regarding PHI as if it applied to TI that is Individually Identifiable.

U.S. Entity/Entities: any corporation, limited liability company, partnership, or other legal entity that meets all of the following requirements:

(1) The entity is organized under the laws of a state or commonwealth of the United States or the federal law of the United States and is subject to the jurisdiction of the United States and the state or commonwealth under which it was formed;

(2) The entity's principal place of business, as determined under federal common law, is in the United States; and

(3) None of the entity's directors, officers, or executives, and none of the owners with a five percent (5%) or greater interest in the entity, are listed on the *Specially Designated Nationals and Blocked Persons List* published by the United States Department of the Treasury's Office of Foreign Asset Control or on the Department of Health and Human Services, Office of Inspector General's List of Excluded Individuals/Entities.

Upstream Subparticipant: a Subparticipant that provides services to a Downstream

Subparticipant pursuant to a Downstream Subparticipant Agreement to send and/or receive information as described in Section 9 of the Common Agreement.

Use(s) (including correlative uses/tenses, such as "Uses," "Used," and "Using"): with respect to TI, means the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

2. Cooperation and Non-Discrimination

2.1 Cooperation. Participant understands and acknowledges that numerous activities with respect to the Framework Agreements will likely involve Alliance, the RCE, other QHINs and their respective Participants and Subparticipants, as well as employees, agents, third-party contractors, vendors, or consultants of each of them. To the extent not in violation of Applicable Law, Participant shall, and shall also require that its Subparticipants incorporate the following obligations into all Framework Agreements to which they are a party, if any:

(i) Respond in a timely manner, as may be further provided in an SOP, to inquiries from Alliance about possible issues related to the exchange of information under the Framework Agreements;

(ii) Participate collaboratively in discussions coordinated by Alliance to address differing interpretations of requirements in the Framework Agreements, the QTF, or any SOP prior to pursuing or, in the case of a Participant, requesting Alliance initiate the TEFCA Dispute Resolution Process as set forth in Section 15.1 of the Common Agreement;

(iii) Make reasonable efforts to notify Alliance when persistent and widespread connectivity failures are occurring with Participant or its Subparticipants, so that all those affected can investigate the problems and identify the root cause(s) of the connectivity failures;

(iv) Work cooperatively, including, without limitation, participating in contact facilitated by Alliance with other QHINs or their Participants or their Subparticipants and facilitate contact with Participant's Subparticipants, to address the root cause(s) of persistent and widespread connectivity failures;

(v) Provide information, or require Participant's Subparticipants to provide information, to Alliance in support of collaborative efforts to resolve issues or disputes, provided that such information is subject to Participant's right to restrict or condition its cooperation or disclosure of information in the interest of preserving privileges in any reasonably foreseeable litigation or protecting Confidential Information;

(vi) Provide information to aid the efforts of Alliance or of other QHINs or their respective Participants or Subparticipants to understand, contain, and mitigate a TEFCA Security Incident at the request of Alliance, provided that such information is subject to Participant's right to restrict or condition its cooperation or disclosure of information in the interest of preserving privileges in any reasonably foreseeable litigation or protecting Confidential Information; and

(vii) Subject to Participant's right to restrict or condition its cooperation or disclosure of information in the interest of preserving privileges in any reasonably foreseeable litigation or protecting Confidential Information, disclose to Alliance information that Participant or Participant's Subparticipants may have that relates to the following:

(a) cybersecurity risk information sharing programs; or

(b) specific, identified security flaws in the operation of the Participant or its Subparticipant(s) that may require the Participant or its Subparticipant(s) to take specific steps to protect the security of their information technology systems and would not otherwise fall into subsection (a).

In no case shall Participant be required to disclose TI or other information in violation of Applicable Law. In seeking cooperation, Alliance and Participant shall make all reasonable efforts to accommodate the other's schedules and reasonable operational concerns. The costs of cooperation to Participant shall not be charged to the RCE or other QHINs. Nothing in this Section 2.1. shall modify or replace the TEFCA Security Incident notification obligations under Section 8.3 and, if applicable, Section 6.5.3 of this Amendment.

2.2 Non-Discrimination.

2.2.1 Prohibition Against Exclusivity. Neither Alliance nor Participant shall prohibit or attempt to prohibit any of Participant's Subparticipant from joining, exchanging with, conducting other transactions with, or supporting any other networks or exchange frameworks, using services *other than* the Connectivity Services, concurrently with the QHIN's, Participant's, or Subparticipant's participation in exchange activities conducted under the Framework Agreements.

2.2.2 No Discriminatory Limits on Exchange of TI. Neither Alliance nor Participant shall impede the exchange of information as permitted or required under the applicable Framework Agreements or limit interoperability with any Participant, Subparticipant, or Individual in a discriminatory manner. As used in this Section 2.2.2, a "discriminatory

manner" means action that is inconsistently taken or not taken with respect to any similarly situated Participant, Subparticipant, Individual, or group of them, whether it is a competitor, or whether it is affiliated with or has a contractual relationship with any other entity, or in response to an event. Notwithstanding the foregoing, limitations, load balancing of network traffic, or other activities, protocols, or rules shall not be deemed discriminatory to the extent that they: (i) satisfy the requirements of the exception set forth in 45 CFR 171.205; and/or (ii) are based on a reasonable and good-faith belief that the other entity or group has not satisfied or will not be able to satisfy the applicable terms hereof (including compliance with Applicable Law) in any material respect, including, if applicable, any Required Flow-Down(s).

2.3 Subparticipant Agreements. Participant shall enter into a Participant-Subparticipant Agreement with each Subparticipant, and shall require Subparticipants to enter a Downstream Subparticipant Agreement with each Downstream Subparticipant.

3. Confidentiality and Accountability

3.1 Confidential Information. Alliance and Participant each agree to use all Confidential Information received pursuant to this Amendment only as authorized in this Amendment and any applicable SOP(s) and solely for the purposes of performing its obligations under this Amendment or the proper exchange of information under the Framework Agreements and for no other purpose. Each Party may act as a Discloser and a Recipient, accordingly. A Recipient will disclose the Confidential Information it receives only to its employees, subcontractors, and agents who require such knowledge and use in the ordinary course and scope of their employment or retention and are obligated to protect the confidentiality of the Discloser's Confidential Information in a manner substantially equivalent to the terms required herein for the treatment of Confidential Information. Otherwise, a Recipient agrees not to disclose the Confidential Information received to anyone except as permitted under this Amendment.

4. RCE Directory

4.1 Utilization of the RCE Directory. The RCE Directory Service shall be used by QHINs, their Participants, and their Subparticipants to create and maintain operational connectivity under the Common Agreement and related Framework Agreements. Alliance is providing Participant with access to, and the right to use, the RCE Directory as contained within its QHIN Directory on the express condition that Participant only use and disclose RCE Directory information as necessary to advance the intended use of the RCE Directory Service or as required by Applicable Law. For example, Participant is permitted to disclose RCE Directory information to the workforce members of its Subparticipant's health information technology vendor who are engaged in assisting the Subparticipant with establishing and maintaining connectivity via the

Framework Agreements. Further, Participant shall not use RCE Directory information for marketing or any form of promotion of its own products and services, unless such use or disclosure is primarily part of an effort by Participant to expand, or otherwise improve, connectivity via the Framework Agreements, and any promotion of Participant's own products or services is only incidental to that primary purpose. In no event shall Participant use or disclose the RCE Directory information in a manner that should be reasonably expected to have a detrimental effect on ONC, the RCE, Alliance, other QHINs and/or their Participants or Subparticipants, or any other individual or organization. For the avoidance of doubt, RCE Directory information is Confidential Information except to the extent such information meets one of the exceptions to the definition of Confidential Information.

5. **TEFCA Exchange Activities.**

In addition to the requirements below, Participant and Participant's Subparticipants may only Request information under the applicable Framework Agreement for a specific Exchange Purpose if Participant or Participant's Subparticipant is the type of person or entity that is described in the definition of the applicable Exchange Purpose. Such a Participant or Participant's Subparticipant may use a Business Associate, agent, or contractor to make such a Request, Use, or Disclosure for the applicable Exchange Purpose. For example, only a Health Care Provider as described in the definition of Treatment (or a Business Associate, agent, or contractor acting on that Health Care Provider's behalf) may Request information for the Exchange Purpose of Treatment.

This Amendment specifies, among other things, the reasons for which information may be Requested and transmitted from one QHIN to another QHIN. Participants and Subparticipants should understand that, despite their participation under a Framework Agreement, Alliance is prohibited from engaging in QHIN-to-QHIN exchange for any purpose other than an Exchange Purpose under the Common Agreement. The RCE recognizes that Alliance may participate in other health information exchange networks and Participant and Participant's Subparticipants also likely participate in other networks, as well as non-network information exchange. The Common Agreement, including the Required Flow-Downs contained in this Amendment, does not affect these other activities or the reasons for which Participants and Subparticipants may request and exchange information within their networks and/or subject to other agreements. Such activities are not in any way limited by the Framework Agreements.

5.1 Uses. Participant may Use TI in any manner that: (1) is not prohibited by Applicable Law; (2) is consistent with Participant's Privacy and Security Notice, if applicable; and (3) is in accordance with Sections 7 and 8 of this Amendment.

5.2 Disclosures. Participant may Disclose TI provided such Disclosure: (1) is not prohibited by Applicable Law; (2) is consistent with Participant's Privacy and Security Notice, if applicable; and (3) is in accordance with Sections 7 and 8 of this Amendment.

5.3 Responses. Participant must support **all** Exchange Purposes and must Respond to all Exchange Purposes that are identified as "required" in the Exchange Purposes SOP. Participant must provide all Required Information that is relevant for a required Exchange Purpose, as may be further specified in an implementation SOP for the applicable Exchange Purpose, in Response to a Request transmitted via QHIN-to-QHIN exchange, unless providing the Required Information is prohibited by Applicable Law or this Amendment or if not providing the Required Information is consistent with all Applicable Law and this Amendment.

5.3.1 Exceptions to Required Responses. Notwithstanding the foregoing, Participant is **permitted but not required** to Respond to a Request transmitted via QHIN-to-QHIN exchange in the circumstances set forth in 5.3.1(i)-(vi) below, provided the Response: (1) is not prohibited by Applicable Law; (2) is consistent with Participant's Privacy and Security Notice, if applicable; and (3) is in accordance with this Amendment.

(i) If Participant is a Public Health Authority;

(ii) If Participant utilizes the Government Benefits Determination Exchange Purpose, including such an agency's agent(s)/contractor(s)

(iii) If the reason asserted for the Request is Individual Access Services and the information would not be required to be provided to an Individual pursuant to 45 CFR § 164.524(a)(2), regardless of whether Participant is a NHE, a Covered Entity, or a Business Associate;

(iv) If the Requested information is not Required Information, provided such response would not otherwise violate the terms of this Amendment;

(v) If Participant is a federal agency, to the extent that the Requested Disclosure of Required Information is not permitted under Applicable Law (e.g., it is Controlled Unclassified Information as defined at 32 CFR Part 2002, and the party requesting it does not comply with the applicable policies and controls that the federal agency adopted to satisfy its requirements); or

(vi) If the Exchange Purpose is authorized but not required at the time of the Request, either under this Amendment or the Exchange Purposes SOP.

5.4 Special Legal Requirements. If and to the extent Applicable Law requires that an Individual either consent to, approve, or provide an authorization for the Use or Disclosure of that Individual's information to Participant, such as a more stringent state law relating to sensitive health information, then Participant shall refrain from the Use or Disclosure of such information in connection with this

Amendment unless such Individual's consent, approval, or authorization has been obtained consistent with the requirements of Applicable Law and Section 7 of this Amendment, including, without limitation, communicated pursuant to the process described in the QTF. Copies of such consent, approval, or authorization shall be maintained and transmitted pursuant to the process described in the QTF by whichever party is required to obtain it under Applicable Law, and Participant may make such copies of the consent, approval, or authorization available electronically to any QHIN, Participant, or Subparticipant in accordance with the QTF and to the extent permitted by Applicable Law. Participant shall maintain written policies and procedures to allow an Individual to revoke such consent, approval, or authorization on a prospective basis. If Participant is an IAS Provider, the foregoing shall not be interpreted to modify, replace, or diminish the requirements set forth in Sections 6 of this Amendment for obtaining an Individual's express written consent.

6. **Individual Access Services**

Nothing in the Privacy and Security Notice or in the Individual's written consent collected by Participant who is an IAS Provider pursuant to Section 6.2 and Section 6.3 may contradict or be inconsistent with any applicable provision of Sections 6 or 7.

6.1 Individual Access Services (IAS) Offering(s). Participant may elect to offer Individual Access Services to any Individual in accordance with the requirements of this section and in accordance with all other provisions of this Amendment. Nothing in this Section 6 shall modify, terminate, or in any way affect an Individual's right of access under the HIPAA Privacy Rule at 45 CFR 164.524 with respect to Alliance, Participant, or Participant's Subparticipant that is a Covered Entity or a Business Associate. Nothing in this Section 6 of this Amendment shall be construed as an exception or excuse for any conduct by Participant that meets the definition of information blocking in 45 CFR 171.103.

6.2 Individual Consent. The Individual requesting Individual Access Services shall be responsible for completing Participant's own supplied form for obtaining Individual express consent in connection with the Individual Access Services, as set forth below. Participant may implement secure electronic means (e.g., secure e-mail, secure web portal) by which an Individual may submit such written consent.

6.3 Written Privacy and Security Notice and Individual Consent.

6.3.1 If Participant offers Individual Access Services, it must develop and make publicly available a written privacy and security notice (the "Privacy and Security Notice"). The Privacy and Security Notice must:

(i) Be publicly accessible and kept current at all times, including updated versions;

(ii) Be shared with an Individual prior to the Individual's

use/receipt of services from Participant;

(iii) Be written in plain language and in a manner calculated to inform the Individual of such privacy practices;

(iv) Include a statement regarding whether and how the Individual's TI may be accessed, exchanged, Used, and/or Disclosed by Participant or by other persons or entities to whom/which Participant Discloses or provides access to the information, including whether the Individual's TI may be sold at any time (including the future);

(v) Include a statement that Participant is required to act in conformance with the Privacy and Security Notice and must protect the security of the information it holds in accordance with Section 6 of this Amendment;

(vi) Include information regarding whom the Individual may contact within Participant for further information regarding the Privacy and Security Notice and/or with privacy-related complaints;

(vii) Include a requirement by Participant to obtain express written consent to the terms of the Privacy and Security Notice from the Individual prior to the access, exchange, Use, or Disclosure (including sale) of the Individual's TI, other than Disclosures that are required by Applicable Law;

(viii) Include information on how the Individual may revoke consent;

(ix) Include an explanation of the Individual's rights, including, at a minimum, the rights set forth in Section 6.4, below;

(x) Include a disclosure of any applicable fees or costs related to IAS including the exercise of rights under Section 6.4 of this Amendment; and

(xi) Include an effective date.

The implementation of such Privacy and Security Notice requirements shall be set forth in the IAS SOP. If Participant is a Covered Entity, then a Notice of Privacy Practices that meets the requirements of 45 CFR § 164.520 **and** meets the requirement of 6.3.1(iv) above can satisfy the Privacy and Security Notice requirements. Nothing in this Section 6.3 reduces a Covered Entity's obligations under the HIPAA Rules.

6.3.2 If Participant is an IAS Provider, it must collect the Individual's written

consent as required under Section 6.3.1 (vii) of this Amendment at the outset of the Individual's first use of the Individual Access Services and with any material change in the applicable Privacy and Security Notice.

6.4 Individual Rights. Individuals have, and must be clearly informed of, the following rights:

(i) The right to require that **all** of their Individually Identifiable information maintained by Participant as an IAS Provider be deleted unless such deletion is prohibited by Applicable Law; provided, however, that the foregoing shall not apply to Individually Identifiable information contained in audit logs.

(ii) The right to an export of their Individually Identifiable information in a computable format, including the means to interpret such information.

The rights described in this Section 6.4 shall control over any inconsistent provisions in Section 7.

6.5 Additional Security Requirements for IAS Providers. In addition to meeting the applicable security requirements set forth in Section 12, if Participant is an IAS Provider, it must further satisfy the requirements of this subsection.

6.5.1 Scope of Security Requirements. If Participant is an IAS Provider, it must comply with the applicable security requirements set forth in this Amendment and applicable security SOPs for **all** Individually Identifiable information they hold, regardless of whether such information is TI.

6.5.2 Encryption. If Participant is an IAS Provider, it is required to encrypt **all** Individually Identifiable information held by Participant, both in transit and at rest, regardless of whether such data are TI.

6.5.3 TEFCA Security Incident Notice to Affected Individuals. Each Participant that is an IAS Provider must notify each Individual whose TI has been or is reasonably believed to have been affected by a TEFCA Security Incident involving the IAS Provider. Such notification must be made without unreasonable delay and in no case later than sixty (60) days following Discovery of the TEFCA Security Incident. The notification required under this section must be written in plain language and shall include, to the extent possible:

(i) A brief description of what happened, including the date of the TEFCA Security Incident and the date of its Discovery, if known;

(ii) A description of the type(s) of Unsecured TI involved in the TEFCA Security Incident (such as whether full name, Social Security number, date of birth, home address, account

number, diagnosis, disability code, or other types of information were involved);

(iii) Any steps Individuals should take to protect themselves from potential harm resulting from the TEFCA Security Incident;

(iv) A brief description of what the Participant involved is doing to investigate the TEFCA Security Incident, to mitigate harm to Individuals, and to protect against any further TEFCA Security Incidents; and

(v) Contact procedures for Individuals to ask questions or learn additional information related to the TEFCA Security Incident, which shall include a telephone number (toll-free), e-mail address, and website with contact information and/or a contact form for the IAS Provider.

To the extent Participant is already required by Applicable Law to notify an Individual of an incident that would also be a TEFCA Security Incident, this section does not require duplicative notification to that Individual.

6.6 Survival for IAS Providers. The following minimum provisions and their respective minimum time periods shall continue to apply to Participant to the extent that it is an IAS Provider and survive expiration or termination of the applicable Framework Agreement under which Individual Access Services were provided for the time periods and to the extent described below.

6.6.1 The following Section 6 provisions shall survive the expiration or termination of the applicable Framework Agreement until expiration of the time period specified in the definition of PHI at 45 CFR § 160.103 under Subsection 2(iv) of such definition, i.e., fifty (50) years after the death of the Individual for whom Individual Access Services were provided, even if the information to which the provisions apply is not ePHI:

(i) The terms of the consent under Section 6.2, Individual Consent, and the terms of the Privacy and Security Notice under Section 6.3.1, which sets forth requirements that apply to the Privacy and Security Notice;

(ii) Section 6.3.2, which requires Participant to collect the Individual's written consent with respect to any material change in the applicable Privacy and Security Notice;

(iii) Section 6.4, Individual Rights; and

6.6.2 Section 6.5, Additional Security Requirements for IAS Providers.

6.6.3 Section 6.5.3, TEFCA Security Incident Notice to Affected Individuals, shall survive for a period of six (6) years following the expiration or termination of the applicable Framework Agreement.

6.7 Provisions that Apply to Subcontractors and Agents of IAS Providers. To the extent that Participant is an IAS Provider and uses subcontractors or agents with respect to the provision of such Individual Access Services, it shall include in a written agreement with each such subcontractor or agent a requirement to comply with the following:

(i) To act in accordance with each of the applicable consents required of Participant under Section 6.2;

(ii) To act in accordance with each of Participant's applicable Written Privacy and Security Notices pursuant to Section 6.3;

(iii) To act in accordance with Section 6.4 when directed to do so by Participant;

(iv) With respect to the information for which the subcontractor or agent provides services to Participant in its role as an IAS Provider, the agent or subcontractor shall implement the applicable security requirements set forth in Sections 8.1 and 8.2 of this Amendment and the applicable security SOPs for **all** such Individually Identifiable information, regardless of whether such information is TI, to the same extent as they apply to Participant.

(v) To encrypt **all** Individually Identifiable information both in transit and at rest, regardless of whether such data are TI pursuant to Section 6.5.2; and

(vi) To notify Participant that is an IAS Provider for which it provides services with respect to each Individual whose TI has been or is reasonably believed to have been affected by a TEFCA Security Incident involving the subcontractor or agent in the manner and within the timeframe specified pursuant to Section 6.5.3.

Each agreement between Participant and a subcontractor or agent with respect to the provision of Individual Access Services shall also provide that subsections through (v) above shall continue in effect after termination or expiration of such agreement at least until expiration of the time period specified in the definition of PHI at 45 CFR § 160.103 under subsection 2(iv) of such definition, i.e., fifty (50) years after the death of the Individual to whom the information relates. Each such agreement shall also provide that subsection (vi) above shall survive for at least six (6) years following the termination or expiration of such agreement.

7. **Privacy**

7.1 Compliance with the HIPAA Privacy Rule. If Participant or Subparticipant is a NHE (but not to the extent that it is acting as an entity entitled to make a Government Benefits Determination under Applicable Law, a Public Health Authority, or a Government Health Care Entity), then it shall comply with the provisions of the HIPAA Privacy Rule listed below with respect to all Individually Identifiable information that Participant or Subparticipant reasonably believes is TI as if such information is Protected Health Information and Participant is a Covered Entity. Such compliance shall be consistent with Section 9 and enforced as part of its obligations pursuant to this Amendment.

7.1.1 From 45 CFR § 164.502, General Rules:

- Subsection (a)(1) – Dealing with permitted Uses and Disclosures**, but only to the extent Participant or Subparticipant is authorized to engage in the activities described in this subsection of the HIPAA Privacy Rule for the applicable Exchange Purpose.**
- Subsection (a)(2)(i) – Requiring Disclosures to Individuals
- Subsection (a)(3) – Business Associates
- Subsection (a)(5) – Dealing with prohibited Uses and Disclosures
- Subsection (b) – Dealing with the Minimum Necessary standard
- Subsection (c) – Dealing with agreed-upon restrictions
- Subsection (d) – Dealing with deidentification and re-identification of information
- Subsection (e) – Dealing with Business Associate contracts
- Subsection (f) – Dealing with deceased persons' information
- Subsection (g) – Dealing with personal representatives
- Subsection (h) – Dealing with confidential communications
- Subsection (i) – Dealing with Uses and Disclosures consistent with notice
- Subsection (j) – Dealing with Disclosures by whistleblowers

7.1.2 45 CFR § 164.504, Organizational Requirements.

7.1.3 45 CFR § 164.508, Authorization Required. Notwithstanding the foregoing, the provisions of Sections 6.2 and 6.3 shall control and this Section 7.1.3 shall not apply with respect to an IAS Provider that is a NHE.

7.1.4 45 CFR § 164.510, Uses and Disclosures Requiring Opportunity to Agree

or Object. Notwithstanding the foregoing, an IAS Provider that is a NHE but is not a Health Care Provider shall not have the right to make the permissive Disclosures described in § 164.510(3) - Emergency circumstances; provided, however, that an IAS Provider is not prohibited from making such a Disclosure if the Individual has consented to the Disclosure pursuant to Section 6 of this Amendment.

7.1.5 45 CFR § 164.512, Authorization or Opportunity to Object Not Required. Notwithstanding the foregoing, an IAS Provider that is a NHE but is not a Health Care Provider shall not have the right to make the permissive Disclosures described in § 164.512(c) - Standard: Disclosures about victims of abuse, neglect or domestic violence, § 164.512 Subsection (d) - Standard: Uses and disclosures for health oversight activities, and § 164.512 Subsection (j) - Standard: Uses and disclosures to avert a serious threat to health or safety; provided, however, that an IAS Provider is not prohibited from making such a Disclosure(s) if the Individual has consented to the Disclosure(s) pursuant to Section 6 of this Amendment.

7.1.6 From 45 CFR § 164.514, Other Requirements Relating to Uses and Disclosures:

- Subsections (a)-(c) – Dealing with de-identification requirements that render information **not** Individually Identifiable for purposes of this Section 6 and TEFCA Security Incidents
- Subsection (d) – Dealing with Minimum Necessary requirements
- Subsection (e) – Dealing with Limited Data Sets

7.1.7 45 CFR § 164.522, Rights to Request Privacy.

7.1.8 45 CFR § 164.524, Access of Individuals **,** except that an IAS Provider that is a NHE shall be subject to the requirements of Section 6 with respect to access by Individuals for purposes of Individual Access Services and not this Section 7.1.8.

7.1.9 45 CFR § 164.528, Accounting of Disclosures.

7.1.10 From 45 CFR § 164.530, Administrative Requirements:

- Subsection (a) – Dealing with personnel designations
- Subsection (b) – Dealing with training
- Subsection (c) – Dealing with safeguards
- Subsection (d) – Dealing with complaints
- Subsection (e) – Dealing with sanctions
- Subsection (f) – Dealing with mitigation

- Subsection (g) – Dealing with refraining from intimidating or retaliatory acts
- Subsection (h) – Dealing with waiver of rights
- Subsection (i) – Dealing with policies and procedures
- Subsection (j) – Dealing with documentation

7.2 Written Privacy Policy. Participant must develop, implement, make publicly available, and act in accordance with a written privacy policy describing its privacy practices with respect to Individually Identifiable information that is Used or Disclosed pursuant to this Amendment. Participant can satisfy the written privacy policy requirement by including applicable content consistent with the HIPAA Rules into its existing privacy policy, except as otherwise stated herein with respect to IAS Providers. This written privacy policy requirement does not supplant the HIPAA Privacy Rule obligations of a QHIN, Participant, or a Subparticipant that is a Covered Entity to post and distribute a Notice of Privacy Practices that meets the requirements of 45 CFR § 164.520. If Participant is a Covered Entity, then this written privacy practices requirement can be satisfied by its Notice of Privacy Practices. If Participant is an IAS Provider, then the written privacy practices requirement **must** be in the form of a Privacy and Security Notice that meets the requirements of Section 6.3 of this Amendment.

8. **Security**

8.1 Security Controls. Participant shall implement and maintain appropriate security controls for TI that are commensurate with risks to the confidentiality, integrity, and/or availability of the TI. If Participant is a NHE, it shall comply with the HIPAA Security Rule provisions with respect to all Individually Identifiable information that Participant reasonably believes is TI as if such information were Protected Health Information and Participant were a Covered Entity or Business Associate. Participant shall comply with any additional security requirements that may be set forth in an SOP applicable to Participants.

8.2 TI Outside the United States. Participant shall not Use TI outside the United States or Disclose TI to any person or entity outside the United States except to the extent such Use or Disclosure is permitted or required by Applicable Law and except to the extent the Use or Disclosure is conducted in conformance with the HIPAA Security Rule, regardless of whether Participant is a Covered Entity or Business Associate. Participant shall evaluate the risks of any extraterritorial Uses and/or Disclosures of TI, if applicable, as part of an annual security assessment and prior to any new or substantially different type of non-U.S. Use(s) or Disclosure(s). Such security assessment shall include a risk assessment to evaluate whether the Uses or Disclosures of Individually Identifiable information that is reasonably believed to be TI by or to persons or entities outside the United States satisfies the requirements of the HIPAA Security Rule. The foregoing does not modify or eliminate any provision of Applicable Law that does not permit Participant to Disclose Individually

Identifiable information to a person or entity outside the United States or that imposes conditions or limitations on such Disclosure.

8.3 TEFCA Security Incident Notification.

8.3.1 Reporting to Alliance. As soon as reasonably practicable, but not more than five (5) calendar days after determining that any TEFCA Security Incident may have occurred, Participant shall provide notification to Alliance of the suspected TEFCA Security Incident. Such notification must include sufficient information for Alliance and others affected to understand the nature and likely scope of the TEFCA Security Incident. Participant shall supplement the information contained in the notification as it becomes available and cooperate with Alliance and, at the direction of Alliance, with the RCE, and with other QHINs, Participants, and Subparticipants that are likely impacted by the TEFCA Security Incident.

8.3.2 Reporting to Subparticipants. Participant shall report any TEFCA Security Incident experienced by or reported to the Participant to all of Participant's Subparticipants. Such notification shall be in accordance with the timing and content requirements stated in Section 8.3.

8.3.3 Vertical Reporting of TEFCA Security Incident(s). Participant shall require that each Subparticipant with which it has entered into a Participant- Subparticipant Agreement:

(i) Report any TEFCA Security Incident experienced by or reported to the Subparticipant to Participant and to the Subparticipant's Downstream Subparticipants, in accordance with the timing and content requirements stated in Section 8.3;

(ii) Require that each Subparticipant with which Participant enters into a Participant-Subparticipant Agreement require that its Downstream Subparticipants report any TEFCA Security Incident experienced by or reported to the Downstream Subparticipant to the Upstream Subparticipant and to its own Downstream Subparticipants, in accordance with the timing and content requirements stated in Section 8.3.

9. General Obligations

9.1 Compliance with Applicable Law and the Framework Agreements. Participant and its Subparticipants shall comply with all Applicable Law and shall implement and act in accordance with any provision required by this Amendment, including all applicable SOPs and provisions of the QTF, which are hereby expressly incorporated into this Amendment. While not every SOP or requirement in the

QTF will be applicable to every Participant or Subparticipant, it is the responsibility of each Participant to determine, in consultation with Alliance, which of the SOPs and QTF provisions are applicable to them. Participant shall be responsible for taking reasonable steps to confirm that all of its Subparticipants are abiding by the terms of this Amendment that are applicable to Subparticipants, specifically including all applicable SOPs and QTF provisions. In the event that Participant becomes aware of a material non-compliance by one of its Subparticipants, then Participant shall promptly notify the Subparticipant in writing. Such notice shall inform the Subparticipant that its failure to correct any such deficiencies within the timeframe established by Participant shall constitute a material breach of the Participant-Subparticipant Agreement, which may result in early termination of said agreement.

9.2 Rights to Suspend.

9.2.1 Suspension Rights Granted to RCE. Participant acknowledges and agrees that the RCE has the authority to suspend any QHIN, Participant, Subparticipant or Downstream Subparticipant's right to engage in any QHIN- to-QHIN exchange activities if: (a) there is an alleged violation of the respective Framework Agreement or of Applicable Law by the respective party/parties; (b) there is a cognizable threat to the security of the information that the RCE reasonably believes is TI transmitted pursuant to such Framework Agreement or to the infrastructure of the respective party; or (c) such suspension is in the interests of national security as directed by an agency of the United States government.

9.2.2 Suspension Rights Granted to Alliance. Participant acknowledges and agrees that Alliance has the same authority as the RCE to suspend Participant, its Subparticipants and their Downstream Subparticipant's right to engage in any activities under the respective Framework Agreement if any of the circumstances described in Subsections 9.2.1 (a)-(c) above occur with respect to Participant, Subparticipant and/or any Downstream Subparticipant of Alliance.

(i) Alliance *may* exercise such right to suspend based on its own determination that any of the circumstances described in Subsections 9.2.1 (a)-(c) above occurred with respect to Participant, Subparticipant and/or any Downstream Subparticipant of Alliance.

(ii) Alliance ***must*** exercise such right to suspend if directed to do so by the RCE based on the RCE's determination that suspension is w Subsections 9.2.1 (a)-(c) above with respect to Participant, Subparticipant and/or any Downstream Subparticipant of Alliance.

9.2.3 Suspension Rights Granted to Participant. In each of its Participant-

Subparticipant Agreements, Participant shall ensure that each Subparticipant agrees and acknowledges that in addition to the suspension authority of the RCE in Subsections 9.2.1 and the Alliance in Subsections 9.2.2, Participant also has the authority to suspend its Subparticipant or Downstream Subparticipant's right to engage in any activities under the respective Framework Agreement if any of the circumstances described in Subsections 9.2.1 (a)-(c)above occur with respect to such Subparticipant or Downstream Subparticipant.

(i) Participant *may* exercise such right to suspend based on its own determination that any of the circumstances described in Subsections 9.2.1 (a)-(c) above occurred with respect to Subparticipant and/or any Downstream Subparticipant of Participant.

(ii) Participant ***must*** exercise such right to suspend if directed to do so by the Alliance. If the suspension is at the direction of Alliance, Participant is required to effectuate such suspension as soon as practicable and not longer than within twenty-four (24) hours of Alliance having directed the suspension, unless Alliance permits a longer period of time in which to effectuate the suspension.

9.2.4 Suspension Rights Granted to Subparticipant. To the extent that a Subparticipant has Downstream Subparticipant, Subparticipant shall reserve the same rights of suspension with respect to such Downstream Subparticipants that Participant has with respect to such Subparticipant pursuant to Subsections 9.2.3.

10. Survival for Participants and Subparticipants.

10.1 Survival for Participants and Subparticipants. The following sections of this Amendment shall survive expiration or termination of this Amendment as more specifically provided below. Further, Participant shall include at least the following survival provisions in all of its Participant-Subparticipant Agreements as Required Flow-Downs so that such provisions will also be included as minimum survival provisions and minimum survival time periods in all Downstream Subparticipant Agreements:

(i) Section 3,Confidential Information, shall survive for a period of six (6) years following the expiration or termination of the applicable Framework Agreement.

(ii) Section 6.6, Survival for IAS Providers, to the extent that Participant or its Subparticipant is an IAS Provider, shall survive following the expiration or termination of the applicable Framework Agreement for

the respective time periods set forth in Section 6.6.

(iii) Section 7, Privacy, to the extent that Participant or its Subparticipant is subject to Section 7, said Section shall survive the expiration or termination of the applicable Framework Agreement until the expiration of the time period specified in the definition of PHI at 45 CFR § 160.103 under Subsection 2(iv) of such definition, i.e., fifty (50) years after the death of the Individual to whom the information covered by Section 7 relates.

(iv) Section 8.1, Security Controls, to the extent that Participant or its Subparticipant is subject to Section 8.1, said Section shall survive the expiration or termination of the applicable Framework Agreement until the expiration of the time period specified in the definition of PHI at 45 CFR § 160.103 under Subsection 2(iv) of such definition, i.e., fifty (50) years after the death of the Individual to whom the information covered by Section 8.1 relates.

(v) The requirements of Section 8.3.1, Vertical Reporting of TEFCA Security Incident(s), shall survive for a period of six (6) years following the expiration or termination of the applicable Framework Agreement.