

**Exhibit 1 to the Common Agreement for Nationwide
Health Information Interoperability**

Participant/Subparticipant Terms of Participation

Version 1.0

April 2024

Effective July 1st, 2024

As a Participant or Subparticipant, You agree to abide by these Participant/Subparticipant Terms of Participation (“ToP”).

1. Definitions and Relevant Terminology.

- 1.1 **Defined Terms.** Capitalized terms used in these ToP shall have the meaning set forth below. 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.

Breach of Unencrypted Individually Identifiable Information: the acquisition, access, or Disclosure of unencrypted Individually Identifiable Information maintained by an IAS Provider that compromises the security or privacy of the unencrypted Individually Identifiable Information.

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 § 164.314(a) and 164.504(e), as applicable.

Common Agreement: unless otherwise expressly indicated, the Common Agreement for Nationwide Health Information Interoperability, 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 CI Discloser, or that a reasonable person would understand to be of a confidential nature, and is disclosed to a CI Recipient pursuant to a Framework Agreement. For the avoidance of doubt, “Confidential Information” does not include electronic protected health information (ePHI), as defined herein, that is subject to a Business Associate Agreement and/or other provisions of a Framework Agreement.

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 CI Recipient; or (ii) is learned by the CI Recipient from a third party that the CI Recipient reasonably believes is entitled to disclose it without restriction; or (iii) is

already known to the CI Recipient before receipt from the CI Discloser, as shown by the CI Recipient's written records; or (iv) is independently developed by CI Recipient without the use of or reference to the CI Discloser's Confidential Information, as shown by the CI Recipient's written records, and was not subject to confidentiality restrictions prior to receipt of such information from the CI Discloser.

Confidential Information (CI) Discloser: a person or entity that discloses Confidential Information.

Confidential Information (CI) Recipient: a person or entity that receives Confidential Information.

Connectivity Services: the technical services provided by a QHIN, Participant, or Subparticipant to its Participants and Subparticipants that facilitate TEFCA Exchange and are consistent with the requirements of the then-applicable QHIN Technical Framework.

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

Designated Network: the Health Information Network that a QHIN uses to offer and provide the Designated Network Services.

Designated Network Governance Body: a representative and participatory group or groups that approve the processes for fulfilling the Governance Functions and participate in such Governance Functions for Signatory's Designated Network.

Designated Network Services: the Connectivity Services and/or Governance Services.

Directory Entry(ies): listing of each Node controlled by a QHIN, Participant or Subparticipant, which includes the endpoint resource for such Node(s) and any other organizational or technical information required by the QTF or an applicable SOP.

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

Discover (including its correlative meanings "Discovery" and "Discovering"): the first day on which something is known to the QHIN, Participant, or Subparticipant, or by exercising reasonable diligence would have been known, to the QHIN, Participant, Subparticipant.

Discriminatory Manner: an act or omission that is inconsistently taken or not taken

with respect to any similarly situated QHIN, 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.

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

Exchange Purpose or XP: means the reason, as authorized by a Framework Agreement, including the applicable SOP(s), for a transmission, Query, Use, Disclosure, or Response transacted through TEFCA Exchange.

Framework Agreement(s): with respect to QHINs, the Common Agreement; and with respect to a Participant or Subparticipant, the ToP.

FTC Rule: the Health Breach Notification Rule promulgated by the Federal Trade Commission set forth at 16 CFR Part 318.

Government Benefits Determination: a determination made by any agency, instrumentality, or other unit of the federal, State, local, or tribal government as to whether an Individual qualifies for government benefits for any purpose other than health care (e.g., 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.

Governance Functions: the functions, activities, and responsibilities of the Designated Network Governance Body as set forth in an applicable SOP.

Governance Services: the governance functions described in an applicable SOP, which are performed by a QHIN's Designated Network Governance Body for its Participants and Subparticipants to facilitate TEFCA Exchange in compliance with the then-applicable requirements of the Framework Agreements.

Health Care Provider: meets the definition of such term in either 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, Pub. Law 104-191 and the Health Information Technology for Economic and Clinical Health Act of 2009, Pub. Law 111-5.

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.

Implementation Date: the date sixty (60) calendar days after publication of version 2 of the Common Agreement in the Federal Register.

Individual: has the meaning assigned to such term at 45 CFR § 171.202(a)(2).

Individual Access Services Incident (IAS Incident): a TEFCA Security Incident or a Breach of Unencrypted Individually Identifiable Information maintained by an IAS Provider.

Individual Access Service Consent (IAS Consent): an IAS Provider's own supplied form for obtaining express written consent from the Individual in connection with the IAS.

Individual Access Services Provider (IAS Provider): each QHIN, Participant, and Subparticipant that offers Individual Access Services (IAS).

Individual Access Services (IAS): the services provided to an Individual by a QHIN, Participant, or Subparticipant that has a direct contractual relationship with such Individual in which the QHIN, Participant, or Subparticipant, as applicable, agrees to satisfy that Individual's ability to use TEFCA Exchange to access, inspect, obtain, or transmit a copy of that Individual's Required Information.

Individually Identifiable Information: 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.

Initiating Node: a Node through which a QHIN, Participant, or Subparticipant initiates transactions for TEFCA Exchange and, to the extent such transaction is a Query, receives a Response to such Query.

Node: a technical system that is controlled directly or indirectly by a QHIN, Participant, or Subparticipant and that is listed in the RCE Directory Service.

Non-HIPAA Entity (NHE): a QHIN, Participant, or Subparticipant that is neither a Covered Entity nor a Business Associate as defined under the HIPAA Rules with regard to activities under a Framework Agreement. To the extent a QHIN, Participant, or Subparticipant is a Hybrid entity, as defined in 45 CFR § 164.103, such QHIN, Participant, or Subparticipant shall be considered a Non-HIPAA Entity with respect to TEFC Exchange activities related to such QHIN, Participant, or Subparticipant's non-covered components.

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

Participant: to the extent permitted by applicable SOP(s), a U.S. Entity that has entered into the ToP in a legally binding contract with a QHIN to use the QHIN's Designated Network Services to participate in TEFC Exchange in compliance with the ToP.

Participant/Subparticipant Terms of Participation (ToP): the requirements set forth in Exhibit 1 to the Common Agreement, as reflected herein, to which: QHINs must contractually obligate their Participants to agree; to which QHINs must contractually obligate their Participants to contractually obligate their Subparticipants and Subparticipants of the Subparticipants to agree, in order to participate in TEFC Exchange including the QHIN Technical Framework (QTF), all applicable Standard Operating Procedures (SOPs), and all other attachments, exhibits, and artifacts incorporated therein by reference.

Privacy and Security Notice: an IAS Provider's own supplied written privacy and security notice that contains the information required by the applicable SOP(s).

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

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

QHIN Technical Framework (QTF): the most recent effective version of the document that contains the technical, functional, privacy, and security requirements for TEFC Exchange.

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.

Query(ies) (including its correlative uses/tenses “Queried” and “Querying”): the act of asking for information through TEFC Exchange.

RCE Directory Service: a technical service provided by the RCE that enables QHINs to identify their Nodes to enable TEFC Exchange. The requirements for use of, inclusion in, and maintenance of the RCE Directory Service are set forth in the Framework Agreements, QTF, and applicable SOPs.

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.

Required Information: the Electronic Health Information, as defined in 45 CFR § 171.102, that is (i) maintained in a Responding Node by any QHIN, Participant, or Subparticipant prior to or during the term of the applicable Framework Agreement and (ii) relevant for a required XP Code, as set forth in the QTF or an applicable SOP(s).

Responding Node: a Node through which the QHIN, Participant, or Subparticipant Responds to a received transaction for TEFC Exchange.

Response(s) (including its correlative uses/tenses “Responds,” “Responded” and “Responding”): the act of providing the information that is the subject of a Query or otherwise transmitting a message in response to a Query through TEFC Exchange.

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 Framework Agreements to provide detailed information or requirements related to TEFC Exchange, including all amendments thereto. Each SOP identifies the relevant group(s) to which the SOP applies, including whether Participants or Subparticipants are required to comply with a given SOP.

State: any of the several States, the District of Columbia, Puerto Rico, the Virgin Islands, Guam, American Samoa, and the Northern Mariana Islands.

Subparticipant: to the extent permitted by applicable SOP(s), a U.S. Entity that has entered into the ToP in a legally binding contract with a Participant or another Subparticipant to use the Participant's or Subparticipant's Connectivity Services to participate in TEFCA Exchange in compliance with the ToP.

TEFCA Exchange: the transaction of information between Nodes using an XP Code.

TEFCA Information (TI): any information that is transacted through TEFCA Exchange except to the extent that such information is received by a QHIN, Participant, or Subparticipant that is a Covered Entity, Business Associate, or NHE that is exempt from compliance with the Privacy section of the applicable Framework Agreement and is incorporated into such recipient's system of records, at which point the information is no longer TI with respect to such recipient and is governed by the HIPAA Rules and other Applicable Law.

TEFCA Security Incident(s):

- (i) An unauthorized acquisition, access, Disclosure, or Use of unencrypted TI using TEFCA Exchange, but **NOT** including any of the following:
 - (a) Any unintentional acquisition, access, Use, or Disclosure of TI by a Workforce Member or person acting under the authority of a QHIN, Participant, or Subparticipant, if such acquisition, access, Use, or Disclosure (i) was made in good faith, (ii) was made by a person acting within their scope of authority, (iii) was made to another Workforce Member or person acting under the authority of any QHIN, Participant, or Subparticipant, and (iv) does not result in further acquisition, access, Use, or Disclosure in a manner not permitted under Applicable Law and the Framework Agreements.
 - (b) 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.
 - (c) A Disclosure of TI that has been de-identified in accordance with the standard at 45 CFR § 164.514(b).
- (ii) Other security events (e.g., ransomware attacks), as set forth in an SOP, that adversely affect a QHIN's, Participant's, or Subparticipant's participation in TEFCA Exchange.

Threat Condition: (i) a breach of a material provision of a Framework Agreement that has not been cured within fifteen (15) days of receiving notice of the material breach (or such other period of time to which the Parties have agreed), which notice shall include such specific information about the breach that the RCE has available at

the time of the notice; or (ii) a TEFCO Security Incident; or (iii) an event that RCE, a QHIN, its Participant, or their Subparticipant has reason to believe will disrupt normal TEFCO Exchange, either due to actual compromise of or the need to mitigate demonstrated vulnerabilities in systems or data of the QHIN, Participant, or Subparticipant, as applicable, or could be replicated in the systems, networks, applications, or data of another QHIN, Participant, or Subparticipant; or (iv) any event that could pose a risk to the interests of national security as directed by an agency of the United States government.

United States: the fifty (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.

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

- (i) 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;
- (ii) The entity's principal place of business, as determined under federal common law, is in the United States; and
- (iii) 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 United States Department of Health and Human Services, Office of Inspector General's *List of Excluded Individuals/Entities*.

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.

Workforce Member(s): any employees, volunteers, trainees, and other persons whose conduct, in the performance of work for an entity, is under the direct control of such entity, whether or not they are paid by the entity.

XP Code: the code used to identify the XP in any given transaction, as set forth in the applicable SOP(s).

1.2 ToP Terminology.

1.2.1 References to You and QHINs, Participants, and Subparticipants. As set forth in its definition and in the introductory paragraph of these ToP, the term “You” is used to refer to the specific entity that is a party to these ToP with the Upstream QPS. (You and Upstream QPS may also be referred to herein individually as a “Party” or collectively as the “Parties.”) Any and all rights and obligations of a QHIN, Participant or Subparticipant stated herein are binding upon all other QHINs, Participants, and Subparticipants that have entered into a Framework Agreement. References herein to “QHINs,” “other Participants,” “other Subparticipants,” and similar such terms are used to refer to any and all other organizations that have signed a Framework Agreement.

1.2.2 General Rule of Construction. For the avoidance of doubt, a reference to a specific section of the ToP in a particular section does not mean that other sections of the ToP that expressly apply to You are inapplicable. A reference in these ToP to any law, any regulation, or to Applicable Law includes any amendment, modification or replacement to such law, regulation, or Applicable Law.

1.2.3 Terms of Participation for Subparticipants. You shall contractually obligate your Subparticipants, if any, to comply with the ToP. Notwithstanding the foregoing, for any entity that became Your Subparticipant prior to the Implementation Date, You shall (i) contractually obligate such entity to comply with the ToP within one-hundred eighty (180) days of the Implementation Date, provided that such Subparticipant is and remains a party to the Participant Subparticipant Agreement, as defined in and required by Common Agreement Version 1.1, during such period; or (ii) terminate such entity’s ability to engage in TEFCA Exchange upon the earlier of the date of termination of the existing Participant-Subparticipant Agreement or one-hundred (180) days after the Implementation Date.

2. **Cooperation and Non-Discrimination.**

2.1 Cooperation. You understand and acknowledge that numerous activities with respect to the ToP will likely involve the RCE, QHINs, and their respective Participants and Subparticipants, as well as employees, agents, third-party contractors, vendors, or consultants of each of them. You shall reasonably cooperate with the RCE, ONC, QHINs and their respective Participants and Subparticipants in all matters related to TEFCA Exchange, including any dispute resolution activities in which You are involved. Expectations for reasonable

cooperation are set forth in an SOP. The costs of cooperation to You shall be borne by You and 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, the IAS Incident notification obligations under Section 6.3.2 of the ToP.

2.2 Non-Discrimination.

- 2.2.1 Prohibition Against Exclusivity. Upstream QPS shall not prohibit or attempt to prohibit You, nor shall You or Upstream QPS prohibit or attempt to prohibit any of Your Subparticipants, if any, from joining, exchanging with, conducting other transactions with, or supporting any other networks or exchange frameworks that use services *other than* the Upstream QPS's Designated Network Services or Your Connectivity Services, concurrently with Your or Your Subparticipants' participation in TEFCA Exchange. Notwithstanding the foregoing, this subsection does not preclude You from including and enforcing reasonable term limits in the contracts with Your Subparticipants related to Your Subparticipants' use of Your Connectivity Services.
- 2.2.2 No Discriminatory Limits on Exchange of TI. Neither You nor Upstream QPS shall engage in TEFCA Exchange, refrain from engaging in TEFCA Exchange, or limit TEFCA Exchange with any QHIN, Participant, Subparticipant, or Individual in a Discriminatory Manner. Notwithstanding the foregoing, if You refrain from engaging in TEFCA Exchange or limit interoperability with any other QHIN, Participant, or Subparticipant under the following circumstances, Your actions or inactions shall not be deemed discriminatory: (i) Your Connectivity Services require load balancing of network traffic or similar activities provided such activities are implemented in a consistent and non-discriminatory manner for a period of time no longer than necessary to address the network traffic issue; (ii) You have a reasonable and good-faith belief that the other QHIN, Participant, or Subparticipant has not satisfied or will not be able to satisfy the applicable terms of a Framework Agreement (including compliance with Applicable Law) in any material respect; and/or (iii) Your actions or inactions are consistent with or permitted by an applicable SOP. One QHIN, Participant, or Subparticipant suspending its exchange activities with another QHIN, Participant, or Subparticipant in accordance with Section 17.4.2 of the Common Agreement or Section 10.4.5 of the ToP, as applicable, shall not be deemed discriminatory.
- 2.2.3 Updates to Connectivity Services. In revising and updating Connectivity Services from time to time, You will use commercially reasonable efforts to

do so in accordance with generally accepted industry practices and to implement any changes in a non-discriminatory manner; provided, however, this provision shall not apply to limit modifications or updates to the extent that such revisions or updates are required by Applicable Law or implemented to respond promptly to newly discovered privacy or security threats.

- 2.2.4 Notice of Updates to Connectivity Services. You shall implement a reporting protocol to provide reasonable prior written notice of all modifications or updates of Your Connectivity Services to Upstream QPS and Your Subparticipants if such revisions or updates are expected to adversely affect Your ability to engage in TEFCA Exchange or require changes in the Connectivity Services of Upstream QPS or Your Subparticipants, regardless of whether they are necessary due to Applicable Law or newly discovered privacy or security threats.

3. Confidentiality and Accountability.

- 3.1 Confidential Information. You and Upstream QPS each agree to use and disclose all Confidential Information received pursuant to these ToP only as authorized in these ToP and any applicable SOP(s) and solely for the purposes of performing its obligations under a Framework Agreement or the proper exchange of information through TEFCA Exchange and for no other purpose. You and Upstream QPS may act as a CI Discloser and a CI Recipient, accordingly. A CI Recipient may disclose the Confidential Information it receives only to its Workforce Members 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 CI Discloser's Confidential Information in a manner substantially equivalent to the terms required herein for the treatment of Confidential Information. If a CI Recipient must disclose the CI Discloser's Confidential Information under operation of law, it may do so provided that, to the extent permitted by Applicable Law, the CI Recipient gives the CI Discloser reasonable notice to allow the CI Discloser to object to such redisclosure, and such redisclosure is made to the minimum extent necessary to comply with Applicable Law.
- 3.2 Disclosure of Confidential Information. Nothing herein shall be interpreted to prohibit Upstream QPS or the RCE from disclosing any Confidential Information to ONC. You acknowledge that ONC, as a Federal government agency, is subject to the Freedom of Information Act. Any disclosure of Your Confidential Information to

ONC or any ONC contractor will be subject to Applicable Law, as well as the limitations, procedures, and other relevant provisions of any applicable SOP(s).

- 3.3 ONC's and the RCE's Approach when Requesting Confidential Information. As a matter of general policy, ONC will request only the limited set of Confidential Information that ONC believes is necessary to inform the specific facts and circumstances of a matter. The RCE will request only the limited set of Confidential Information that the RCE believes is necessary to inform the specific facts and circumstances of a matter.

4. RCE Directory Service and Directory Entries.

- 4.1 Utilization of Directory Entries. The RCE Directory Service and Directory Entries contained therein shall be used by QHINs solely as necessary to create and maintain operational connectivity to enable TEFCA Exchange. Upstream QPS is providing You with access to, and the right to use, Directory Entries on the express condition that You only use and disclose Directory Entry information as necessary to advance the intended use of the Directory Entries or as required by Applicable Law. For example, You are permitted to disclose Directory Entry information to Your Workforce Members, Your Subparticipant's Workforce Members, and/or to the Workforce Members of health information technology vendors who are engaged in assisting You or Your Subparticipant with establishing and maintaining connectivity via the Framework Agreements. Further, You shall not use another QPS's Directory Entries or information derived therefrom for marketing or any form of promotion of Your own products and services, unless otherwise permitted pursuant to an SOP. In no event shall You use or disclose the information contained in the Directory Entries in a manner that should be reasonably expected to have a detrimental effect on ONC, the RCE, Upstream QPS, Your Subparticipants, other QHINs, other Participants, other Subparticipants, or any other individual or organization. For the avoidance of doubt, Directory Entries are Confidential Information of the CI Discloser except to the extent such information meets one of the exceptions to the definition of Confidential Information. Nothing herein shall be interpreted to prohibit a QHIN or Upstream QPS from publicly disclosing the identity of its own Participants or Subparticipants.
- 4.2 Top Record. You must maintain a record of all ToPs into which You enter with Your Subparticipants, if any, regardless of whether such Subparticipants are listed in the RCE Directory Services. Such record must be provided to the RCE within four (4) business days following the RCE's or Upstream QPS's written request unless such other timeframe is agreed to by the RCE.

5. TEFCA Exchange Activities.

- 5.1 Utilization of TEFCA Exchange. You may only utilize Connectivity Services for purposes of facilitating TEFCA Exchange. You may only utilize TEFCA Exchange for an XP. To the extent there are limitations on what types of Participants or Subparticipants may transact TEFCA Information for a specific XP, such limitations will be set forth in the applicable SOP(s). All TEFCA Exchange is governed by and must comply with the Framework Agreements governing the QHINs, Participants, and Subparticipants engaging in the TEFCA Exchange.

To the extent that Upstream QPS provides you with access to other health information exchange networks, these ToP do not affect these other activities or the reasons for which You may request and exchange information within these other networks. Such activities are not in any way limited by the Framework Agreements provided the transactions are not TEFCA Exchange.

- 5.2 Uses. You may Use TI in any manner that: (i) is not prohibited by Applicable Law; (ii) is consistent with Your Privacy and Security Notice, if applicable; and (iii) is in accordance with Sections 7 and 8 of these ToP.
- 5.3 Disclosures. You may Disclose TI provided such Disclosure: (i) is not prohibited by Applicable Law; (ii) is consistent with Your Privacy and Security Notice, if applicable; and (iii) is in accordance with Sections 7 and 8 of these ToP.
- 5.4 Responses. Except as otherwise set forth in an applicable SOP, Your Responding Nodes must Respond to Queries for all XP Codes that are identified as “required.” in the applicable SOP(s). Such Response must include all Required Information. Notwithstanding the foregoing, You may withhold some or all of the Required Information to the extent necessary to comply with Applicable Law.
- 5.5 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 You, such as a more stringent federal or State law relating to sensitive health information, then You shall refrain from the Use or Disclosure of such information in connection with these ToP unless such Individual’s consent, approval, or authorization has been obtained consistent with the requirements of Applicable Law and Section 7 of these ToP, including, without limitation, communicated pursuant to the access consent policy(ies) described in the QTF or applicable SOP(s). 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 You 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. You shall maintain written policies and procedures to allow an Individual to revoke such consent, approval, or authorization on a prospective basis. If You are an IAS Provider, the foregoing shall not be interpreted to modify, replace, or diminish the requirements set forth in Section 6 of these ToP and any applicable SOP(s) for obtaining an Individual's express written consent.

6. Individual Access Services.

- 6.1 IAS Offering(s). You may elect to be an IAS Provider by offering IAS to any Individual in accordance with the requirements of this section and in accordance with all other provisions of these ToP and applicable SOP(s). 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 if You are a Covered Entity or a Business Associate. Nothing in this Section 6 of these ToP shall be construed as modifying or taking precedence over any provision codified in 45 CFR Part 171. An IAS Provider shall not prohibit or attempt to prohibit any Individual using the IAS of any other IAS Provider or from joining, exchanging with, conducting other transactions with any other networks or exchange frameworks, using services *other than* the IAS Providers' Designated Network Services, concurrently with the QHIN's, Participant's, or Subparticipant's participation in TEFCA Exchange.
- 6.2 Individual Consent. This Section 6.2 shall apply to You if You are an IAS Provider. The Individual requesting IAS shall be responsible for completing the IAS Consent. The IAS Consent shall include, at a minimum: (i) consent to use the IAS; (ii) the Individual's acknowledgement and agreement to Your Privacy and Security Notice; and (iii) a description of the Individual's rights to access, delete, and export such Individual's Individually Identifiable Information. You may implement secure electronic means (e.g., secure e-mail, secure web portal) by which an Individual may submit the IAS Consent. You shall collect the IAS Consent prior to the Individual's first use of the IAS and prior to any subsequent use if there is any material change in the applicable IAS Consent, including the version of the Privacy and Security Notice referenced therein. Nothing in the IAS Consent may contradict or be inconsistent with any applicable provision of these ToP or the SOP(s). If You are a Covered Entity and have a Notice of Privacy Practices that meets the requirements of 45 CFR § 164.520, You are not required to have a Privacy and Security Notice that meets the requirements of the applicable SOP. Nothing in Section 6 reduces a Covered Entity's obligations under the HIPAA Rules.

- 6.3 Additional Security Requirements for IAS Providers. In addition to meeting the applicable security requirements set forth in Section 8, if You are an IAS Provider, You must further satisfy the requirements of this subsection.
- 6.3.1 Scope of Security Requirements. You must meet the applicable security requirements set forth in Section 8 for **all** Individually Identifiable Information You maintain as an IAS Provider, regardless of whether such information is TI.
- 6.3.2 IAS Incident Notice to Affected Individuals. If You reasonably believe that an Individual has been affected by an IAS Incident, You must provide such Individual with notification without unreasonable delay and in no case later than sixty (60) days following Discovery of the IAS Incident. The notification required under this section must be written in plain language and shall include, to the extent possible, the information set forth in the applicable SOP(s). To the extent You are already required by Applicable Law to notify an Individual of an incident that would also be an IAS Incident, this section does not require duplicative notification to that Individual.
- 6.4 Survival for IAS Providers. This Section 6.4 shall apply to You if You are an IAS Provider. As between You as an IAS Provider and an Individual, the IAS Provider's obligations in the IAS Consent, including Your requirement to comply with the Privacy and Security Notice and provide Individuals with rights, shall survive for so long as You maintain such Individual's Individually Identifiable Information. If You were an IAS Provider, the requirements of Section 6.3 shall survive termination of these ToP for so long as You maintain Individually Identifiable Information acquired during the term of these ToP as an IAS Provider regardless of whether such information is or was TI.

7. Privacy.

- 7.1 Compliance with the HIPAA Privacy Rule. If You are a NHE (but not to the extent that You are acting as an entity entitled to make a Government Benefits Determination under Applicable Law, a Public Health Authority, or a Government Health Care Entity or any other type of entity exempted from compliance with this Section in an applicable SOP), then You shall comply with the provisions of the HIPAA Privacy Rule listed below with respect to all Individually Identifiable

information as if such information is Protected Health Information and You are a Covered Entity.

7.1.1 From 45 CFR § 164.502, General Rules:

- Subsection (a)(1) – Dealing with permitted Uses and Disclosures, **but only to the extent You are authorized to engage in the activities described in this subsection of the HIPAA Privacy Rule for the applicable XP.**
- Subsection (a)(2)(i) – Requiring Disclosures to Individuals
- 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 de-identification 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(e), Organizational Requirements.

7.1.3 45 CFR § 164.508, Authorization Required. Notwithstanding the foregoing, the provisions of Sections 6.2 shall control and this Section 7.1.3 shall not apply with respect to You if You are 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(a)(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 these ToP.

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 these ToP.

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 Information for purposes of this Section 7 and TECCA 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 Protections.

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 IAS 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. You must develop, implement, make publicly available, and act in accordance with a written privacy policy describing Your privacy practices with respect to Individually Identifiable Information that is Used or Disclosed pursuant to these ToP. You can satisfy the written privacy policy requirement by including applicable content consistent with the HIPAA Rules in Your existing privacy policy, except as otherwise stated herein with respect to IAS Providers. If You are a Covered Entity, this written privacy policy requirement does not supplant the HIPAA Privacy Rule obligations to post and distribute a Notice of Privacy Practices that meets the requirements of 45 CFR § 164.520. If You are a Covered Entity, then this written privacy policy requirement can be satisfied by Your Notice of Privacy Practices. If You are 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 6.2 of these ToP. Notwithstanding Section 11.1, to the extent the Signatory’s written privacy policy is “more stringent” than the HIPAA Privacy Rule provisions listed below, the written privacy policy shall govern. “More stringent” shall have the meaning assigned to it in 45 CFR § 160.202 except the written privacy policy shall be substituted for references to State law and the reference to “standards, requirements or implementation specifications adopted under subpart E of part 164 of this subchapter” shall be limited to those listed below.

8. Security.

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

8.2 TEFCA Security Incident Reporting.

8.2.1 Reporting to Upstream QPS. You shall report to Upstream QPS any suspected TEFCA Security Incident, as set forth in the applicable SOP(s). Such report must include sufficient information for Upstream QPS and others affected to understand the nature and likely scope of the TEFCA Security Incident. You shall supplement the information contained in the report as additional relevant information becomes available and cooperate with Upstream QPS and, at the direction of Upstream QPS, with the RCE, and with

other QHINs, Participants, and Subparticipants that are likely impacted by the TEFCA Security Incident.

- 8.2.2 Reporting to Subparticipants. You shall report any TEFCA Security Incident experienced by or reported to You to Your Subparticipants as required by an applicable SOP.
- 8.2.3 Compliance with Notification Under Applicable Law. Nothing in this Section 8.3 shall be deemed to modify or replace any breach notification requirements that You may have under the HIPAA Rules, the FTC Rule, or other Applicable Law. To the extent You are already required by Applicable Law to notify Upstream QPS or a Subparticipant of an incident that would also be a TEFCA Security Incident, this section does not require duplicative notification.
- 8.3 Security Resource Support to Subparticipants. You shall make available to Your Subparticipants (if any): (i) security resources and guidance regarding the protection of TI applicable to the Subparticipants' participation in TEFCA Exchange; and (ii) information and resources that the RCE or Cybersecurity Council makes available to You related to promotion and enhancement of the security of TI under the Framework Agreements.
- 8.4 TI Outside the United States. You shall only Use TI outside the United States or Disclose TI to any person or entity outside the United States to the extent such Use or Disclosure is permitted or required by Applicable Law and the Use or Disclosure is conducted in conformance with the HIPAA Security Rule, regardless of whether You are a Covered Entity or Business Associate and as set forth in an applicable SOP.
- 8.5 Encryption. If You are a NHE (but not to the extent that You are a federal agency or any other type of entity exempted from compliance with this Section in an applicable SOP), You must encrypt all Individually Identifiable Information You maintain, both in transit and at rest, regardless of whether such information is TI. Requirements for encryption may be set forth in an SOP.

9. General Obligations.

- 9.1 Compliance with Applicable Law and the ToP. You shall comply with all Applicable Law and shall implement and act in accordance with any provision required by the ToP, including all applicable SOPs and provisions of the QTF, when engaging in or facilitating TEFCA Exchange. While each SOP identifies the relevant group(s) to which it applies, not every requirement in an SOP or the QTF will necessarily be

applicable to You. It is Your responsibility to determine, in consultation with Upstream QPS, which of the SOPs and QTF provisions are applicable to You.

- 9.2 Your Responsibility for Your Subparticipants. You shall be responsible for taking reasonable steps to confirm that all of Your Subparticipants (if any) are abiding by the ToP, specifically including all applicable SOPs and QTF provisions. In the event that You become aware of a material non-compliance by one of Your Subparticipants, then You shall promptly notify the Subparticipant in writing. Such notice shall inform the Subparticipant that its failure to correct any such deficiencies within thirty (30) days of receiving notice shall constitute a material breach of the ToP, which may result in early termination of these ToP.
- 9.3 Your Responsibility for Your Third-Party Technology Vendors. To the extent that You use a third-party technology vendor that will have access to TEFCa Information in connection with Connectivity Services or TEFCa Exchange, You shall include in a written agreement with each such subcontractor or agent a requirement to comply with all applicable provisions of these ToP and a prohibition on engaging in any act or omission that would cause You to violate the terms of these ToP if You had engaged in such act or omission Yourself.
- 9.4 Fees Charged by QHINs, Participants, or Subparticipants. You may charge fees to an Initiating Node when Responding to Queries through TEFCa Exchange as defined in an applicable SOP. The foregoing shall not prohibit You from charging Your Subparticipants fees for use of Your Connectivity Services.

10. Term, Termination, and Suspension.

- 10.1 Term. These ToP shall become effective upon agreement of both Parties and shall remain in effect until terminated by either Party. You may terminate these ToP by providing at least thirty (30) days' prior written notice of termination to Upstream QPS. Upstream QPS may terminate these ToP by providing at least ninety (90) days' prior written notice to You. Notwithstanding the foregoing, in the event that Upstream QPS's Framework Agreement is terminated, Your ToP shall be immediately terminated.
- 10.2 Termination for Cause. Either Party may terminate these ToP for cause if the other Party commits a material breach of a Framework Agreement, and fails to cure its material breach within thirty (30) days of receiving notice specifying the nature of such breach in reasonable detail from the non-breaching Party; provided, however, that if Upstream QPS is diligently working to cure its material breach at the end of this thirty (30) day period, then You must provide Upstream QPS with up to another thirty (30) days to complete its cure.

- 10.3 Effect of Termination. Upon termination of these ToP, You will no longer be able to engage in TEFCA Exchange facilitated by or through Upstream QPS. To the extent You store TI, such TI may not be distinguishable from other information maintained by You. When the TI is not distinguishable from other information, it is not possible for You to return or destroy TI You maintain upon termination or expiration of these ToP. Upon termination or expiration of these ToP, if You are subject to Section 7 of these ToP, such sections shall continue to apply so long as the information would be ePHI if maintained by a Covered Entity or Business Associate. The protections required under the HIPAA Security Rule shall also continue to apply to all TI that is ePHI, regardless of whether You are a Covered Entity or Business Associate. The provisions set forth in this Section 10.3 are in addition to those survival provisions set forth in Section 11.9.
- 10.4 Conflict with Other Agreements Between You and Upstream QPS. Notwithstanding anything herein to the contrary, in the event You and Upstream QPS are parties to an agreement that provides additional terms related to TEFCA Exchange and that agreement provides for a shorter notice period for termination, such shorter notice period shall control.
- 10.5 Rights to Suspend.
- 10.5.1 RCE's Right to Suspend Your Ability to Engage in TEFCA Exchange. You acknowledge and agree that the RCE has the authority to suspend, or direct the Upstream QPS to suspend, any QPS's ability to engage in TEFCA Exchange if: (i) there is an alleged violation of the respective Framework Agreement or of Applicable Law by the respective party/parties; (ii) there is a Threat Condition; (iii) the RCE determines that the safety or security of any person or the privacy or security of TI and/or Confidential Information is threatened; (iv) such suspension is in the interests of national security as directed by an agency of the United States government; or (v) there is a situation in which the RCE may suffer material harm and suspension is the only reasonable step that the RCE can take to protect itself. You acknowledge that upon receiving direction from the RCE, You will be suspended as soon as practicable provided, however, if the suspension is based on Subsections 10.5.1(i) or 10.5.1(iv) or a Threat Condition that results in a cognizable threat to the security of TEFCA Exchange or the information that the RCE reasonably believes is TI, then You will be suspended within twenty-four (24) hours of the RCE having directed Your QHIN to effectuate the suspension, unless the RCE specifies a longer period of time is permitted.

10.5.2 Upstream QPS's Right to Suspend Your Ability to Engage in TEFCA Exchange.

You acknowledge and agree that Upstream QPS has the same authority as the RCE to suspend Your ability to engage in TEFCA Exchange, and Your Subparticipant's (if any) ability to engage in TEFCA Exchange, if any of the circumstances described in Subsections 10.5.1 (i)-(iii) above occur with respect to You or any of Your Subparticipants.

- (i) Upstream QPS *may* exercise such right to suspend based on its own determination that any of the circumstances described in Subsections 10.5.1 (i)-(iii) above occurred with respect to You or any of Your Subparticipants.
- (ii) Upstream QPS **must** exercise such right to suspend if directed to do so by the RCE or its Upstream QPS based on its determination that suspension is warranted based on any of the circumstances described in Subsections 10.5.1 (i)-(v) above with respect to You or any of Your Subparticipants.
- (iii) You acknowledge that if Upstream QPS makes a determination that suspension is warranted or receives direction from its Upstream QPS to suspend Your ability to engage in TEFCA Exchange, You will be suspended as soon as practicable provided, however, if the suspension is based on the circumstances described in Subsections 10.5.1(i) or 10.5.1(iv) or a Threat Condition that results in a cognizable threat to the security of TEFCA Exchange or the information that the RCE reasonably believes is TI, then You will be suspended within twenty-four (24) hours of notice of Upstream QPS's determination or receipt of direction from its Upstream QPS, unless Upstream QPS specifies a longer period of time is permitted.

10.5.3 Upstream QPS Suspension. Notwithstanding the foregoing, in the event that Upstream QPS's ability to engage in TEFCA Exchange is suspended, Your and any of Your Subparticipants' ability to engage in TEFCA Exchange will be immediately suspended.

10.5.4 Suspension Rights Granted to You Related to Your Subparticipants. If You have Subparticipants, You acknowledge and agree that You have the same responsibility and authority to suspend Your Subparticipant's ability to engage in TEFCA Exchange if any of the circumstances described in Subsections 10.5.1 (i)-(iii) above occur with respect to any of Your Subparticipants. If You make a determination to suspend, You are required

to promptly notify Upstream QPS of Your decision and the reason(s) for making the decision. If any of Your Subparticipants notify You of their decision to suspend exchange with their Subparticipant(s), You must notify Upstream QPS of such decision.

- (i) You *may* exercise such right to suspend based on Your own determination that any of the circumstances described in Subsections 10.5.1 (i)-(iii) above occurred with respect to any of Your Subparticipants.
- (ii) You **must** exercise such right to suspend if directed to do so, by the RCE or Upstream QPS based on the RCE's determination that suspension is warranted based on any of the circumstances described in Subsections 10.5.1 (i)-(v) above with respect to any of Your Subparticipants.
- (iii) You must effectuate such suspension of Your Subparticipant as soon as practicable provided, however, if the suspension is based on the circumstances described in Subsections 10.5.1(i) or 10.5.1(iv) or a Threat Condition that results in a cognizable threat to the security of TEFCA Exchange or the information that the RCE reasonably believes is TI, then it must be effectuated within twenty-four (24) hours of the triggering event, unless a longer period of time is permitted. For purposes of this subsection, the triggering event is Your determination to suspend, Your receipt of direction from your Upstream QPS to suspend, or the RCE having directed Your QHIN to effectuate the suspension.

10.5.5 Selective Suspension. You may, in good faith and to the extent permitted by Applicable Law, determine that You must suspend exchanging with a QHIN, Participant, or Subparticipant with which You are otherwise required to exchange in accordance with an SOP because of reasonable and legitimate concerns related to the privacy, security, accuracy, or quality of information that is exchanged. If You make this determination, You are required to promptly notify Upstream QPS of Your decision and the reason(s) for making the decision. If any of Your Subparticipants notify You of their decision to suspend exchange with a QHIN, Participant, or Subparticipant, You must notify Upstream QPS of such decision. You acknowledge that You may be required to engage in a process facilitated by the RCE to resolve whatever issues led to the decision to suspend. Provided that You selectively suspend exchanging with another QHIN, Participant, or Subparticipant in accordance with this section and in accordance with Applicable Law, such selective

suspension shall not be deemed a violation of Section 2.2 of these ToP.

11. Contract Administration.

- 11.1 Authority to Agree. You warrant and represent that You have the full power and authority to enter into these ToP.
- 11.2 Assignment. None of these ToP can be transferred by either Party, including whether by assignment, merger, other operation of law, change of control (i.e., sale of substantially all of the assets of the Party) of the Party or otherwise, without the prior written approval of the other Party.
- 11.3 Severability. If any provision of these ToP shall be adjudged by any court of competent jurisdiction to be unenforceable or invalid, that provision shall be struck from the ToP, and the remaining provisions of these ToP shall remain in full force and effect and enforceable.
- 11.4 Captions. Captions appearing in these ToP are for convenience only and shall not be deemed to explain, limit, or amplify the provisions of these ToP.
- 11.5 Independent Parties. Nothing contained in these ToP shall be deemed or construed as creating a joint venture or partnership between Upstream QPS and You.
- 11.6 Acts of Contractors and Agents. To the extent that the acts or omissions of a Party's agent(s) or contractor(s), or their subcontractor(s), result in that Party's breach of and liability under these ToP, said breach shall be deemed to be a breach by that Party.
- 11.7 Waiver. The failure of either Party to enforce, at any time, any provision of these ToP shall not be construed to be a waiver of such provision, nor shall it in any way affect the validity of these ToP or any part hereof or the right of such Party thereafter to enforce each and every such provision. No waiver of any breach of these ToP shall be held to constitute a waiver of any other or subsequent breach, nor shall any delay by either Party to exercise any right under these ToP operate as a waiver of any such right.
- 11.8 Priority. In the event of any conflict or inconsistency between any other agreement that You and Upstream QPS enter into with respect to TEFCA Exchange, Applicable Law, a provision of these ToP, the QTF, an SOP, and/or any implementation plans, guidance documents, or other materials or documentation the RCE makes available to QHINs, Participants, and/or Subparticipants regarding the operations or activities conducted under the Framework Agreements, the following shall be the order of

precedence for these ToP to the extent of such conflict or inconsistency: (1) Applicable Law; (2) these ToP; (3) the QTF; (4) the SOPs; (5) all other attachments, exhibits, and artifacts incorporated herein by reference; (6) other RCE plans, documents, or materials made available regarding activities conducted under the Framework Agreements; and (7) any other agreement that You and Upstream QPS enter into with respect to TEFCA Exchange.

11.9 Survival. The following sections of these ToP shall survive expiration or termination of these ToP as more specifically provided below:

- (i) Section 3, Confidentiality and Accountability shall survive for a period of six (6) years following the expiration or termination of these ToP.
- (ii) Section 6.4, Survival for IAS Providers, to the extent that You are an IAS Provider, shall survive following the expiration or termination of these ToP for the respective time periods set forth in Section 6.4.
- (iii) Section 7, Privacy, to the extent that You are subject to Section 7, said Section shall survive the expiration or termination of these ToP so long as the information maintained by You would be ePHI if maintained by a Covered Entity or Business Associate.
- (iv) Section 8.1 Security Controls, and Section 8.5, Encryption, to the extent that You are subject to Sections 8.1 and 8.5, said Section or Sections shall survive the expiration or termination of these ToP for so long as the information maintained by You would be ePHI if maintained by a Covered Entity or Business Associate regardless of whether You are a Covered Entity or Business Associate.
- (v) The requirements of Section 8.2, TEFCA Security Incidents Reporting, shall survive for a period of six (6) years following the expiration or termination of these ToP.