Exhibit 3

TEFCA

If HIN connects to a Qualified Health Information Network (a "QHIN") or becomes a QHIN, as that term is defined in the Trusted Exchange Framework and Common Agreement ("TEFCA"), then the TEFCA Flow Down Terms as follow shall apply.

TEFCA Flow Down Terms

The following definitions will apply only for purposes of this Attachment. Capitalized terms used in this Attachment but not otherwise defined will have the meaning set forth in the Agreement.

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

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 Attachment. For the avoidance of doubt, "Confidential Information" does not include electronic protected health information (ePHI), as defined in this Attachment, that is subject to a Business Associate Agreement and/or other provisions of this Attachment. 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.

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

Direct Relationship: a relationship between (i) an Individual User and (ii) a Party or Participant Member, that arises when the Party or Participant Member, as applicable, offers services to the Individual User in connection with the Agreement, and the Individual User 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.

Dispute: means (i) a disagreement about any provision of this Attachment, 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 Participant, the RCE, or any other Participant Member.

Downstream Subparticipant: a Participant Member that has entered into a Participant Member Agreement to use the services of another Participant Member (referred to as the "Upstream Subparticipant") to send and/or receive information as described in Section 4 of this Attachment.

Downstream Subparticipant Agreement: an agreement that incorporates all of the Required Flow-Downs of this Attachment 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 4 of this Attachment 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 this Attachment 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 this Attachment including the Exchange Purposes SOP, for a Request, Use, Disclosure, or Response transmitted via HIN 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 provisions of this Attachment, and, if applicable, under the implementation SOP for the applicable Exchange Purpose.

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 User 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 Individual Users 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.

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.

IAS Provider: Any Party or Participant Member that offers Individual Access Services.

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

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

Non-HIPAA Entity (NHE): a Party or a Participant Member that is neither a Covered Entity nor a Business Associate under HIPAA with regard to activities under this Attachment.

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.

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 Agreement.

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

QHIN Technical Framework (QTF): the document described in Section 5.2 of this Attachment and incorporated by reference into this Attachment, as may be amended, that may include: (i) technical requirements, functional requirements, and privacy- and security-related requirements for the exchange of TI between HIN and other QHINs; (ii) internal-QHIN functional requirements; (iii) technical, privacy, and security flow-down requirements from the QHIN to Participants and/or

Participant Members (if any) in addition to the privacy and security Required Flow-Downs in this Attachment; and (iv) operational requirements that enable the exchange of TI between and among QHINs.

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

Recognized Coordinating Entity (RCE): the entity selected by ONC that will enter into an agreement with QHINs in order to impose, at a minimum, the requirements of TEFCA, 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 Agreement.

Required Flow-Down(s): the rights and obligations set forth within this Attachment that Participant is required to include in its Participant Member Agreements and that Participant must require Participant Members to obligate Subparticipants to impose on their Downstream Subparticipants, if any, through their Downstream Subparticipant Agreements. Participant is required to include all provisions of this Attachment in its participant Member Agreement for Exchange Purposes.

Required Information:

Electronic information maintained by HIN, Participant, or Subparticipant prior to or during the term of the 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 HIN.

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 Agreement.

Standard Operating Procedure(s) or **SOP(s):** a written procedure or other provision that is adopted pursuant to the agreement in place between HIN and the QHIN or HIN and the RCE (the

"**Common Agreement**") and incorporated by reference into this Attachment 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 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.

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 Member Agreement to use the services of Participant as described in Section 4 of this Attachment 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 4 of this Attachment 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 agreement. As a matter of general policy, once TI is received by HIN, Participant, or a Participant Member 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):

(i) An unauthorized acquisition, access, Disclosure, or Use of unencrypted TI in transit using the Interface or pursuant to this Attachment, between Participant and Participant Members and their Subparticipants, or between Subparticipants, but **NOT** including the following:

(a) Any unintentional acquisition, access, or Use of TI by a workforce member or person acting under the authority of HIN, Participant, or Participant Member, 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 this Attachment.

(b) Any inadvertent Disclosure by a person who is authorized to access TI at HIN, Participant, or Participant Member to another person authorized to access TI at the same HIN, Participant, or Participant Member, or Organized Health Care Arrangement in which HIN, Participant, or Participant Member 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 this Attachment.

(c) A Disclosure of TI where HIN, Participant, or Participant Member 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.

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

(ii) Other security events (e.g., ransomware attacks), as set forth in an SOP, that prevent the affected HIN, Participant, or Participant Member from responding to requests for information as required under this Attachment or otherwise adversely affect their participation in QHIN-to-QHIN exchange.

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 4 of this Attachment.

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.

1. Cooperation and Non-Discrimination

1.1. **Cooperation**. To the extent not in violation of Applicable Law, Participant shall, and shall also incorporate the following obligations into all Participant Member Agreements to which it is a party, if any:

1.1.1. Respond in a timely manner, as may be further provided in an SOP, to inquiries from the RCE or other Participant Members about possible issues related to their exchange of information under this Attachment;

1.1.2. Participate collaboratively in discussions coordinated by the RCE to address differing interpretations of requirements in this Attachment, the QTF, or any SOP prior to pursuing any dispute resolution process;

1.1.3. Make reasonable efforts to notify the RCE and other QHINs, as appropriate, when persistent and widespread connectivity failures are occurring with Participant or Participant Members, so that all those affected can investigate the problems and identify the root cause(s) of the connectivity failures;

1.1.4. Work cooperatively with HIN and other organizations to address the root cause(s) of persistent and widespread connectivity failures;

1.1.5. Provide information (or require its Participant Members) to other Participant Members 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;

1.1.6. Provide information to aid the efforts of other Participant Members or their respective Participant Member End Users to understand, contain, and mitigate a TEFCA Security Incident at the request of such other Participant Members or their respective Participant Member End Users, 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

1.1.7. 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 the RCE information that Participant 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 that may require Participant Members 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, Participant shall make all reasonable efforts to accommodate the other Participant Members' schedules and reasonable operational concerns. The costs of cooperation to Participant shall be borne by Participant and shall not be charged to the RCE or other Participant Members. Nothing in this Section shall modify or replace the TEFCA Security Incident notification obligations under Section 7.3 and, if applicable, Section 5.5.3 of this Attachment.

1.2. Non-Discrimination.

1.2.1. Prohibition Against Exclusivity. Participant shall not prohibit or attempt to prohibit any Participant Members or Participant Member End User from joining, exchanging with, conducting other transactions with, or supporting any other networks or exchange frameworks, using services other than the Interface, concurrently with the Participant's participation in exchange activities conducted under the Agreement.

1.2.2. No Discriminatory Limits on Exchange of TI. Participant shall not impede the exchange of information as permitted or required under the Agreement or limit interoperability with any other Participant Members, Participant Member End User, or Individual User in a discriminatory manner. As used in this Section 1.2.2, a "discriminatory manner" means action that is inconsistently taken or not taken with respect to any similarly situated Participant Members, Participant Members End Users, Individual User, 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. Confidentiality and Accountability

2.1. Confidential Information. Participant agrees to use all Confidential Information received pursuant to this Attachment only as authorized in the Agreement and any applicable SOP(s) and solely for the purposes of performing its obligations under this Attachment or the proper exchange of information under this Attachment and for no other purpose. Participant 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 Attachment.

3. RCE Directory

3.1. Utilization of the RCE Directory Service. The RCE Directory Service shall be used by Participant to create and maintain operational connectivity under the Common Agreement. HIN is providing Participant with access to, and the right to use, the RCE Directory Service on the express condition that Participant only use and disclose information contained in the RCE Directory Service 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 information contained in the RCE Directory Service to the workforce members of its health information technology vendor who are engaged in assisting the Participant with establishing and maintaining connectivity via the Agreement. Further, Participant shall not use the information contained in the RCE Directory Service 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 this Attachment, 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 information contained in the RCE Directory Service in a manner that should be reasonably expected to have a detrimental effect on ONC, the RCE, other Participant Members and/or their Participant Member End Users, or any other individual or organization. For the avoidance of doubt, information contained in the RCE Directory is Confidential Information except to the extent such information meets one of the exceptions to the definition of Confidential Information.

4. TEFCA Exchange Activities

In addition to the requirements below, Participant may only Request information under the Agreement for a specific Exchange Purpose if the Participant Member is the type of person or entity that is described in the definition of the applicable Exchange Purpose. Such Participant Member 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 Attachment specifies, among other things, the reasons for which information may be Requested and transmitted from one Participant Member to another Participant Member. Participant understands that, despite its participation under the Agreement, HIN is prohibited from engaging in exchange for any purpose other than an Exchange Purpose under this Attachment.

4.1. Uses. Signatory may Use TI in any manner that: (i) is not prohibited by Applicable Law; (ii) is consistent with Participant's Privacy and Security Notice, if applicable; and (iii) is in accordance with Sections 6 and 7 of this Attachment, if applicable.

4.2. Disclosures. Participant may Disclose TI provided such Disclosure: (i) is not prohibited by Applicable Law; (ii) is consistent with Participant's Privacy and Security Notice, if applicable; and (iii) is in accordance with Sections 6 and 7 of this Attachment, if applicable.

4.3. 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 HIN to Participant Member exchange, unless providing the Required Information is prohibited by Applicable Law or this Attachment or if not providing the Required Information is consistent with all Applicable Law and this Attachment.

4.3.1. Exceptions to Required Responses. Notwithstanding the foregoing, Participant is permitted but not required to Respond to a Request transmitted via HIN-to-Participant Member exchange in the circumstances set forth in 4.3.1(i)-(vi) below, provided the Response: (a) is not prohibited by Applicable Law; (b) is consistent with Participant's Privacy and Security Notice, if applicable; and (c) is in accordance with this Attachment.

(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 User 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 Attachment;

(v) If Signatory 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 Attachment or the Exchange Purposes SOP.

4.4. Special Legal Requirements. If and to the extent Applicable Law requires that an Individual User either consent to, approve, or provide an authorization for the Use or Disclosure of that Individual User'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 Attachment unless such Individual User's consent, approval, or authorization has been obtained consistent with the requirements of Applicable Law and Section 6 of this Attachment, 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 Participant Member in accordance with the QTF and to the extent permitted by Applicable Law. Participant shall maintain written policies and procedures to allow an Individual User 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 Section 5 of this Attachment for obtaining an Individual User's express written consent.

5. Individual Access Services

Nothing in the Privacy and Security Notice or in the Individual User's written consent collected by Participant who is an IAS Provider pursuant to Section 5.2 and Section 5.3 may contradict or be inconsistent with any applicable provision of Sections 5 or 6.

5.1. Individual Access Services (IAS) Offering(s). Participant may elect to offer Individual Access Services to any Individual Participant in accordance with the requirements of this section and in accordance with all other provisions of this Attachment. Nothing in this Section 5 shall modify, terminate, or in any way affect an Individual User's right of access under the HIPAA Privacy Rule at 45 CFR 164.524 with respect to any Participant Member that is a Covered Entity or a Business Associate. Nothing in this Section 5 of this Attachment shall be construed as an exception or excuse for any conduct by the Participant that meets the definition of information blocking in 45 CFR 171.103.

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

5.3. Written Privacy and Security Notice and Individual Consent.

5.3.1. 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 User prior to the Individual User's use/receipt of services from Participant;

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

(iv) Include a statement regarding whether and how the Individual User'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 5 of this Attachment;

(vi) Include information regarding whom the Individual User 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 User prior to the access, exchange, Use, or Disclosure (including sale) of the Individual User's TI, other than Disclosures that are required by Applicable Law;

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

(ix) Include an explanation of the Individual User's rights, including, at a minimum, the rights set forth in Section 5.4, below;

(x) Include a disclosure of any applicable fees or costs related to IAS including the exercise of rights under Section 5.4 of this Attachment; 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 5.3.1(iv) above can satisfy the Privacy and Security Notice requirements. Nothing in this Section 5.3 reduces a Covered Entity's obligations under the HIPAA Rules.

5.3.2. If Signatory is an IAS Provider, it must collect the Individual's written consent as required under Section 10.3.1(vii) of this Attachment 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.

5.4. Individual Rights. Individual Users 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 5.4 shall control over any inconsistent provisions in Section 6.

5.5. Additional Security Requirements for IAS Providers. In addition to meeting the applicable security requirements set forth in Section 7, if Participant is an IAS Provider it must further satisfy the requirements of this subsection.

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

5.5.2. 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.

5.5.3. TEFCA Security Incident Notice to Affected Individual Users. If Participant is an IAS Provider it must notify each Individual User 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 Individual Users 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 User of an incident that would also be a TEFCA Security Incident, this section does not require duplicative notification to that Individual user.

5.6. 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 Agreement under which Individual Access Services were provided for the time periods and to the extent described below.

5.6.1. The following Section 5 provisions shall survive the expiration or termination of the 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 User 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 5.2, Individual Consent, and the terms of the Privacy and Security Notice under Section 5.3.1, which sets forth requirements that apply to the Privacy and Security Notice;

(ii) Section 5.3.2, which requires Participant to collect the Individual User's written consent with respect to any material change in the applicable Privacy and Security Notice;

(iii) Section 5.4, Individual Rights; and

(iv) Section 5.5, Additional Security Requirements for IAS Providers.

5.6.2. Section 5.5.3, TEFCA Security Incident Notice to Affected Individual Users, shall survive for a period of six (6) years following the expiration or termination of the Agreement.

5.7. 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 5.2;

(ii) To act in accordance with each of Participant's applicable Written Privacy and Security Notices pursuant to Section 5.3;

(iii)To act in accordance with Section 5.4 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 this Attachment (other than Sections 7.1.5, 7.1.6 and 7.3) and the security SOPs for all such Individually Identifiable information, regardless of whether such information is TI, to the same extent as they apply to Participant; provided, however, that for purposes of the Flow-Down Provisions of this Section 5.7, if the IAS Provider is a Participant or Participant member, only Sections 7.1.4 and 7.2 shall apply;

(v) To encrypt all Individually Identifiable information both in transit and at rest, regardless of whether such data are TI pursuant to Section 5.5.2; and

(vi)To notify Participant that is an IAS Provider for which it provides services with respect to each Individual User 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 5.5.3.

Each agreement between Participant and a subcontractor or agent with respect to the provision of Individual Access Services shall also provide that subsections (i) 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.

6. Privacy

6.1. Compliance with the HIPAA Privacy Rule. If Participant 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 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 8.2 (Compliance with Specific Obligations) and enforced as part of its obligations pursuant to this Attachment.

6.1.1. From 45 CFR § 164.502, General Rules:

· Subsection (a)(1) – Dealing with permitted Uses and Disclosures, but only to the extent Participant 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

6.1.2. 45 CFR § 164.504, Organizational Requirements.

6.1.3. 45 CFR § 164.508, Authorization Required. Notwithstanding the foregoing, the provisions of Sections 5.2 and 5.3 shall control and this Section 6.1.3 shall not apply with respect to an IAS Provider that is a NHE.

6.1.4. 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 User has consented to the Disclosure pursuant to Section 5 of this Attachment.

6.1.5. 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 User has consented to the Disclosure(s) pursuant to Section 5 of this Attachment.

6.1.6. 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

6.1.7. 45 CFR § 164.522, Rights to Request Privacy Protections.

6.1.8. 45 CFR § 164.524, Access of Individuals, except that an IAS Provider that is a NHE shall be subject to the requirements of Section 5 with respect to access by Individual Users for purposes of Individual Access Services and not this Section 6.1.8.

6.1.9. 45 CFR § 164.528, Accounting of Disclosures.

6.1.10. 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

6.2. 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 Attachment. 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 Participant 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 5.3 of this Attachment.

7. Security

7.1. Participant shall implement and maintain, and require its Participant Members to 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 be required to comply with the HIPAA Security Rule provisions with respect to all Individually Identifiable information that the Participant reasonably believes is TI as if such information were Protected Health Information and the Participant were a Covered Entity or Business Associate. Participant shall implement and maintain, and require that its Participant Members implement and maintain, any additional security requirements that may be set forth in an SOP applicable to Participants and Participant Members. Such compliance shall be enforced as part of the Participants obligations pursuant to Agreement.

7.2. TI Outside the United States (Required Flow-Down). 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.

7.3. Vertical Reporting of TEFCA Security Incident(s). Participant will:

(i) Notify HIN and Participant Members of any TEFCA Security Incident the Participant experiences as soon as reasonably practicable, but not more than five (5) calendar days after determining that a TEFCA Security Incident has occurred;

(ii) Require that each Participant Member with which Participant enters into a Participant Member Agreement report any TEFCA Security Incident experienced by or

reported to the Participant Member to the Participant and to the Participant Member's Downstream Subparticipants in accordance with the timing and content requirements stated in this Section;

(iii) Require that each Participant Member with which the Participant enters into a Participant Member 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 this Section.

(iv) Notify HIN of any TEFCA Security Incident reported to the Participant by one of its Participant Members.

8. General Obligations

8.1. Compliance with Applicable Law and the Agreement. Participant shall comply with all Applicable Law and shall implement and act in accordance with any provision required by this Attachment, including all applicable SOPs and provisions of the QTF.

8.2. Flow-Down Rights to Suspend.

8.2.1. Suspension Rights Granted. Participant grants authority to the RCE and HIN to suspend Participant's right to engage in any exchange activities under this Attachment if: (i) there is an alleged violation of such agreement or of Applicable Law by the party/parties; (ii) there is a cognizable threat to the security of the information that the RCE reasonably believes is TI transmitted pursuant to such agreement or to the infrastructure of the any Participant Member; or (iii) such suspension is in the interests of national security as directed by an agency of the United States government. Participant shall include the same rights of suspension in its Participant Member Agreement.

8.3. Survival. The following terms shall survive as set forth below and Participant shall include the following minimal survival provisions in its Participant Member Agreement.

8.3.1. Section 2.1, Confidential Information, shall survive for a period of six (6) years following the expiration or termination of the Agreement.

8.3.2. Section 5.6, Survival for IAS Providers, to the extent that Participant is an IAS Provider, shall survive following the expiration or termination of the Agreement for the respective time periods set forth in Section 5.6.

8.3.3. Section 6, Privacy, to the extent that the Participant is subject to Section 6, said Section shall survive the expiration or termination of the 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 6 relates.

8.3.4. Section 7.1, to the extent that Participant is subject to Section 7.1, said Section shall survive the expiration or termination of the 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 7.1 relates.

8.3.5. The requirements of Section 7.3, Vertical Reporting of TEFCA Security Incident(s), shall survive for a period of six (6) years following the expiration or termination of the Agreement.

9. Compliance with Standard Operation Procedures. Participant will comply with all applicable Standard Operating Procedures related to this Attachment and will cause its Participant Members to so agree.

10. Participant shall be responsible for incorporating any Required Flow-Downs into all Participant Member Agreements.