Effective Date: XX/XX/XXXX
Last Revision Date: NA
QHIN Governance Committee Approval Date: xx/xx/xxxx

8300 Boone Blvd., Suite 500, Vienna, Virginia, 22182

EHEALTH EXCHANGE TEFCA INDIVIDUAL ACCESS SERVICES PROTOCOL

Scope and Authority

This Protocol addresses the requirements for Individual Access Services (IAS) that all eHealth Exchange QHIN Participants and any and all levels of Subparticipants must comply with to initiate and respond to IAS requests. Initiating IAS requests is optional. Responding to any IAS request is required.

The eHealth Exchange Coordinating Committee, which is the governing body of the eHealth Exchange, has established the QGC as a standing subcommittee with the authority specified in the Onboarding and Designation SOP, the eHealth Exchange QHIN TEFCA Terms and Conditions and this Protocol. The QGC will have responsibility, oversight, control, and final decision-making authority over each of the Governance Functions: (i) Technical framework of the Designated Network; (ii) The resolution of disputes regarding use of eHealth Exchange QHIN; (iii) eHealth Exchange QHIN Security Incident(s); (iv) enforcement of eHealth Exchange QHIN Participant compliance with all flow-down requirements, and: (v) change management to implement changes for the eHealth Exchange QHIN.

In accordance with eHealth Exchange Operating Policy & Procedures (OPP) #10 (Participant Opt-Out of New Data Sharing Agreements), this protocol applies to all Participants that do not opt-out of the eHealth Exchange QHIN and are thus bound by the TEFCA Terms and Conditions.

Purpose

The primary purpose of this protocol is to provide the requirements for IAS Services by eHealth Exchange QHIN Participants and any and all level of Subparticipants. The QHIN Technical Framework requires eHealth Exchange QHIN Participants and all levels of Subparticipants to meet the IAS initiating request requirements herein if they opt to provide the ability for IAS requests. All eHealth Exchange QHIN Participants and any and all levels of Subparticipants must meet the requirements for responding to IAS request.

Protocol

This protocol addresses the IAS requirements to participate in the eHealth Exchange QHIN. Thus, each eHealth Exchange QHIN Participant and any/all levels of Subparticipants has the obligation to implement processes and procedures to meet the requirements and to initiate, if this service is offered by the Participant or any/all levels of Subparticipants, and respond to all IAS requests.

EHEALTH EXCHANGE TEFCA INDIVIDUAL ACCESS SERVICES PROTOCOL

a. Nothing in this Protocol shall modify, terminate, or in any way affect an Individual's right of access under the HIPAA Privacy Rule in 45 DFR 164.534, where applicable.

The QGC or its Designee, Healtheway, Inc. (d/b/a/ "The eHealth Exchange" and its "eHealth Exchange QHIN support staff"), will conduct periodic reviews to evaluate and identify improvements to the TEFCA Security Incident notification process.

Procedure

Responding to IAS Queries (Required)

1. The eHealth Exchange TEFCA Terms and Conditions requires your organization to respond to request for data asserting the IAS Purpose of Use , as defined in the Common Agreement, as long as Applicable Law permits.
    a. All eHealth Exchange QHIN Participants and any/all levels of Subparticipants that receive a QHIN Query for IAS Exchange Purpose that provides the information specified and provides an acceptable match based on the responder policy are quired to Respond with the Required Information. A responder's determination of a patient match shall not require **more than** the following demographics, unless required by applicable law:
        i. Verification must include, at a minimum; (1) First Name (2) Last Name, (3) Date of Birth, (4) Address, (5) City, (6) State, and (7) Zip Code.
        ii. Verification should also include, but does not require; (1) Sex, (2), Middle Name or Middle Initial, (3) Suffix, (4) Email Address, (5) Mobile Phone Number, (6) Social Security Number (SSN) or SSN last four (4) digits, (7) Medical Record Number, and (8) other identifiers.
2. eHealth Exchange QHIN Participants and all levels of Subparticipants **MUST** Process IAS Requests without the validated attribute SAML codes using the SOAP fault code of urn:oasis:names:tc:SAML:2.0:status:AuthnFailed.

Initiating IAS Queries (Optional)

eHealth Exchange Participant or any/all levels of Subparticipants **MAY** elect to offer IAS to any Individual in accordance with the requirements in this Protocol and in accordance with all other provisions of the eHealth Exchange TEFCA Terms and Conditions.

1. eHealth Exchange QHIN Participants and Subparticipants **MUST** use an RCE approved Credential Service Provider (CSP).
    a. The CSP **MUST** identity proof Individuals to NIST 800-63A Identity Assurance Level 2 (IAL2) including the following prescriptive procedures for evidence collection, validation, and verification for remote or in-person identity proofing. Additional details for NIST 800 63A can be found at https://pages.nist.gov/800-63-3/sp800-63a.html.

EHEALTH EXCHANGE TEFCA INDIVIDUAL ACCESS SERVICES PROTOCOL

a. IAS Providers **MUST** verify the identities of Individuals via a CSP prior to the Individual's first use of Connectivity Services, and then again, each time the credentials expire.
    i. Verification must include, at a minimum; (1) First Name (2) Last Name, (3) Date of Birth, (4) Address, (5) City, (6) State, and (7) Zip Code.
    ii. Verification should also include, but does not require; (1) Sex, (2), Middle Name or Middle Initial, (3) Suffix, (4) Email Address, (5) Mobile Phone Number, (6) Social Security Number (SSN) or SSN last four (4) digits, (7) Medical Record Number, and (8) other identifiers.
        1. IAS Providers **MUST** use the following demographic codes for any validated demographics supplied: First Name 'fname', Last Name 'lname', Middle Name 'mname', Middle Initial 'minitial', Suffix 'suffix', Date of Birth 'dob', Sex 'sex', Address 'address', City 'city', State 'state', ZIP/ZIP+4 'zip', Phone Number 'phone', Email Address 'email', Social Security Number 'ssn', SSN last 4 digits 'ssn4', Medical Record Number 'mrn', Identifier 'identifier'.
        2. IAS Providers supplying validated historical demographic codes **MUST** prepend the code name with a "h". Secondary historical demographic code names must be appended by a mononically increasing integer starting with "2". Example first historical lname would be "hlname", and the second historical lname would be "hlname2".
        3. IAS Providers **MUST** submit queries only using CSP IAL2 validated demographics. a) Historical demographics MAY be included if CSP IAL2 validated. b) Historical demographics must be marked as historical as per section 1.a.ii.2.

b. IAS Providers **MUST** demonstrate that all Individuals are identity proofed to NIST IAL2. The proof of identity verification is included in the QHIN Query or QHIN Message Delivery request SAML via a <saml:AttributeStatement> tag set which includes: i) <saml:Attribute name="csp" NameFormat=""> comprising the Business Name or URL of the CSP and, ii) saml:Attribute name="validated_attributes" NameFormat=""> with a comma or space separated list of the user demographics and identifiers that have been verified by the CSP.
    i. IAS Providers **MAY** include in its QHIN Query or QHIN Message Delivery a token provided by the CSP asserting IAL2 verification of the Individual has been completed.

2. Individual Consent
    a. eHealth Exchange QHIN Participant's or any/all levels of Subparticipant's MUST ensure the Individual requesting IAS has completed the eHealth Exchange QHIN Participant or Subparticipant own supplied form for obtaining express consent in connection with the IAS offering.

b. eHealth Exchange QHIN Participant or Subparticipant may implement secure electronic means (e.g., secure email, secure web portal) by which an Individual may submit such written consent.

3. Written Privacy and Security Notice and Individual Consent

a. If an eHealth Exchange QHIN Participant or any level of Subparticipant offers IAS, Participant/Subparticipant must develop and make publicly available a written privacy and security notice (the "Privacy and Security Notice"). The Privacy and Security Notice must:

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

(ii) Be shared with an Individual prior to the Individual's use/receipt of IAS from Participant;

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

(iv) Include a statement regarding whether and how the Individual's TEFCA Information (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 10 of the eHealth Exchange TEFCA Terms and Conditions;

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

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

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

(ix) Include an explanation of the Individual's rights, including, at a minimum, the rights set forth in Section 3, below;

(x) Include a disclosure of any applicable fees or costs related to IAS including the exercise of rights under Section 10.4 of the TEFCA Terms and Conditions; and

(xi) Include an effective date.

b. The implementation of such Privacy and Security Notice requirements shall be in accordance with the IAS Privacy and Security Notice SOP, including as may be amended by the Recognized Coordinating Entity (RCE). If eHealth Exchange QHIN Participant/Subparticipant is a Covered Entity, then a Notice of Privacy Practices that meets the requirements of 45 CFR § 164.520 and meets the requirement of 2(a)(iv) above can satisfy the Privacy and Security Notice requirements. Nothing in this Section reduces a Covered Entity's obligations under the HIPAA Rules.

c. If the eHealth Exchange QHIN Participant/Subparticipant is an IAS Provider, it must collect the Individual's written consent as required under this Protocol and the eHealth Exchange TEFCA Terms and Conditions at the outset of the Individual's first use of IAS and with any material change in the applicable Privacy and Security Notice.

4. Individual Rights

Individuals have, and must be clearly informed of, the following rights:

a. The right to require that all of their Individually Identifiable information maintained by an eHealth Exchange Participant/Subparticipant 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.

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

5. Additional Security Requirements for IAS Providers

eHealth Exchange QHIN Participants and Subparticipants that offer IAS must satisfy the additional requirements:

a. If the eHealth Exchange QHIN Participant or Subparticipant is an IAS Provider, it must comply with the applicable security requirements set forth in the eHealth Exchange TEFCA Terms and Conditions and applicable security SOPs for ALL Individually Identifiable information they hold, regardless of whether such information is TI.

b. If the eHealth Exchange QHIN Participant or Subparticipant is an IAS Provider, it is required to encrypt ALL Individually Identifiable information held by the QHIN Participant or Subparticipant, both in transit and at rest, regardless of whether such data are TI.

c. Each eHealth Exchange QHIN Participant or Subparticipant which is an IAS Provider, must notify each Individual whose TI has been or is reasonably believed to have been affected by a TEFCA Security Incident involving the IAS Provider. In addition to following the eHealth Exchange TEFCA Security Incident Protocol, the following must be followed:

i. Such notification must be made without unreasonable delay and in no case later

than sixty (60) days following Discovery of the TEFCA Security Incident.

ii. 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, if known, and the date of its Discovery;

(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 IAS Provider involved is doing to investigate the TEFCA Security Incident, to mitigate harm to Individuals, and to protect against any further TEFCA Security Incidents; and

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

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

6. Survival for IAS Providers

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

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

(i) The terms of the consent under Section 1, Individual Consent, and the terms of the Privacy and Security Notice under Section 2 which sets forth requirements that apply to the Privacy and Security Notice;

(ii) Section 2.c. which requires an IAS Provider to collect the Individual's written consent with respect to any material change in the applicable Privacy and Security Notice;

(iii) Section 3, Individual Rights; and

(iv) Section 4, Additional Security Requirements for IAS Providers.

Section 4, TEFCA Security Incident Notice to Affected Individuals, shall survive for a period of six (6) years following the expiration or termination of the applicable Framework Agreement.

7. Provisions that Apply to Subcontractors and Agents of IAS Providers

To the extent that an eHealth Exchange QHIN Participant or any level of Subparticipant that is an IAS Provider uses subcontractors or agents with respect to the provision of such Individual Access Services, the IAS Provider shall include in a written agreement with each such subcontractor or agent a requirement to comply with the following:

a. To act in accordance with each of the applicable consents required of the eHealth Exchange QHIN Participant or Subparticipant IAS Provider under Section 2;
b. To act in accordance with each of the eHealth Exchange QHIN Participant or Subparticipant IAS Provider's applicable written Privacy and Security Notices pursuant to Section 3;
c. To act in accordance with Section 4 when directed to do so by the eHealth Exchange Participant or Subparticipant IAS Provider;
d. With respect to the information for which the subcontractor or agent provides services to the eHealth Exchange QHIN Participant or Subparticipant in its role as an IAS Provider, the agent or subcontractor shall implement the applicable security requirements set forth in Sections 12.1 and 12.2 of the TEFCA Terms and the applicable security SOPs for **all** such Individually Identifiable information, regardless whether such information is TI, to the same extent as they apply to eHealth Exchange QHIN Participant or Subparticipant.
e. To encrypt **all** Individually Identifiable information both in transit and at rest, regardless of whether such data are TI pursuant to Section 5.b; and
f. To notify the eHealth Exchange QHIN Participant or Subparticipant IAS Provider for which it provides services with respect to each Individual whose TI has been or is reasonably believed to have been affected by a TEFCA Security Incident involving the subcontractor or agent in the manner and within the timeframe specified pursuant to Section 5.c.

Each agreement between the eHealth Exchange QHIN Participant or any level of Subparticipant that is an IAS Provider and a subcontractor or agent with respect to the provision of IAS 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

(f) above shall survive for at least six (6) years following the termination or expiration of such agreement.

8. Non-Permitted Permissive Disclosures

eHealth Exchange QHIN Participants and and any level of Subparticipant that is an IAS Providers that are Non-HIPAA Entities and are not Health Care Providers do not have the right to issue a Permissive Disclosure under 45 CFR 164.150(3) and 45 CFR 164.512 (c), (d), or (j) unless that Individual has consented.

Definitions

All capitalized terms, if not defined herein, shall have the same meaning as set forth in the TEFCA Terms & Conditions or the TEFCA Protocols.

References

"Qualified Health Information Network (QHIN) Technical Framework (QTF) Version 1"

- https://rce.sequoiaproject.org/tefca-and-rce-resources/

"Recognized Coordinating Entity (RCE), Standard Operating Procedure: Exchange Purposes"

- https://rce.sequoiaproject.org/tefca-and-rce-resources/

"Recognized Coordinating Entity (RCE), Standard Operating Procedure: IAS Exchange Purpose Implementation"

- https://rce.sequoiaproject.org/tefca-and-rce-resources/

Related Protocols

"eHealth Exchange TEFCA Enforcement Protocol"

ID	Date	Author	Comments
		Pat Russell	Initial Protocol