ONC TEFCA RECOGNIZED COORDINATING ENTITY

Standard Operating Procedure (SOP): Individual Access Service (IAS) Provider Requirements

Version 2.0

DRAFT for Stakeholder Feedback

January 19, 2024

Applicability: QHINs, Participants, or Subparticipants that offer Individual Access Services (IAS Providers)

1 Common Agreement References

The requirements set forth in this Standard Operating Procedure (SOP) are required for implementation in addition to the terms and conditions found in the Common Agreement, the Qualified Health Information Network™ (QHIN™) Technical Framework (QTF), and applicable SOPs. The Trusted Exchange Framework and Common Agreement℠ (TEFCA℠) Cross Reference Resource identifies which SOPs provide additional detail on specific references from the Common Agreement.

All documents cited in this SOP can be found on the Recognized Coordinating Entity® (RCE™) website.

2 SOP Definitions

Terms defined in this section are introduced herein and can be found in the TEFCA Glossary. Capitalized terms used in this SOP without definition shall have the respective meanings assigned to such term in the TEFCA Glossary.

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

3 Purpose

TEFCA enables Individuals to access their Individually Identifiable information via an IAS Provider's application, website, or other interface. To support such access, it is imperative that the Common Agreement promote trust and transparency in how Individually Identifiable information is protected and safeguarded.

Section 10 of the Common Agreement outlines terms and conditions that IAS Providers must follow to offer IAS. Among other things, IAS Providers are required to obtain the Individual's express written consent in connection with IAS, including acknowledgment of and agreement to the IAS Provider's written Privacy and Security Notice that describes the privacy and security practices used to safeguard Individually Identifiable information.[1]

Section 10 also requires IAS Providers to notify Individuals of a TEFCA Security Incident or a Breach of Unencrypted Individually Identifiable Information maintained by the IAS Provider (IAS Incident).

[1] Nothing in this SOP alters a Covered Entity's obligations under the HIPAA Rules.

This SOP contains additional details regarding the content of the Privacy and Security Notice, as well as requirements for notifying Individuals of an IAS Incident. Requirements that fall under the Exchange Purpose (XP) Implementation SOP: Demographics Matched are out of scope for this SOP.

4 PROCEDURE

4.1 Written Privacy and Security Notice and Individual Consent

IAS Providers are required to have a publicly available, written Privacy and Security Notice (for purposes of this SOP "Notice") that provides an explanation, as described below, of the privacy and security practices of the IAS Provider with respect to Individually Identifiable information and the Individual's rights with respect to their Individually Identifiable information maintained by the IAS Provider in connection with the Individual Access Services.

a. IAS Providers must implement the Notice using the following standards. The Notice must meet each of the following requirements:

1. Be publicly accessible and kept current at all times, including updated versions.
    a. The IAS Provider also must:
        i. Conspicuously post and make available the Notice on any website and user facing application the IAS Provider maintains where the website or user-facing application is related to the IAS it offers or provides information about its IAS customer services;
        ii. Conspicuously post any changes to the Notice on the IAS Provider's website and user-facing application no later than the effective date of the change to the Notice; and
        iii. Proactively make reasonable efforts to ensure that Individuals already enrolled with the IAS Provider receive an updated version of the Notice with any material changes, consistent with the following:
            1. The updated version must be provided in accordance with the Individual's communicated preferences;
            2. Material changes to the Notice should be conspicuously displayed in such a way as to allow Individuals to readily identify changes in the updated version; and
            3. In the event of a dispute regarding whether an IAS Provider should have made reasonable efforts to proactively notify Individuals of a change to the Notice, the IAS Provider has the burden to prove the change was immaterial.

2. Be shared with an Individual prior to the Individual's use/receipt of IAS from the IAS Provider.
    a. The IAS Provider also must:
        i. Provide the Notice in a manner that allows the Individual to reach out to the IAS Provider with questions; and
        ii. Provide the Notice in electronic form.

3. Be written in plain language and in a manner calculated to inform the Individual of such privacy practices.
    a. The IAS Provider also must:
        i. Reasonably comply with the latest version of the Federal Plain Language Guidelines;[2]
        ii. At least, include the words "Privacy and Security Notice" in the Notice title;
        iii. Translate the Notice into any non-English language that is the primary language of at least five (5) percent of the individual users in the IAS Provider's service area[3];
        iv. Use a format that makes the policy readable, including on smaller screens such as a mobile device:
            1. Use graphics or icons to help readers easily recognize privacy and security practices and settings.

4. Include a statement regarding whether and how Individually Identifiable information may be accessed, exchanged, Used, and/or Disclosed by IAS Provider or by other persons or entities to whom/which IAS Provider Discloses or provides access to the information, including whether the Individually Identifiable information may be sold at any time (including the future).
    a. The statement also must clearly explain:
        i. That Individually Identifiable information cannot be accessed, exchanged, Used, and/or Disclosed by the IAS Provider to assert any type of claim against the Individual by the IAS Provider except for the collection of fees;
        ii. If Individually Identifiable information may be further accessed by, exchanged with, Used by and/or Disclosed to third parties;

[2] Federal plain language guidelines available at https://www.plainlanguage.gov/guidelines/.
[3] Contract Year 2021 Translated Model Materials Requirements and Language Data Analysis Methodology available at https://www.hhs.gov/guidance/sites/default/files/hhs-guidance-documents//cy2021_translated_model_materials_requirements_and_language_data_analysis_methodology.pdf.

iii. The types of persons/entities to which the Individually Identifiable information may be further Disclosed and Used, if any, including ways that may be outside of the IAS Provider's control;

iv. The period of time for which the IAS Provider will retain the Individually Identifiable information;

v. The specific purpose for any Use of Individually Identifiable information, subject to Section 11.1 of the Common Agreement. The purpose must be described with sufficient detail for Individuals to understand how the data will be used (e.g., if the data is being sold, including to downstream entities, or is being exchanged for something of value, now or in the future, such detail must be made clear to the user[4]). Any direct Disclosures to the Individual do not require such an explanation in the Notice;

vi. Whether the IAS Provider will de-identify Individually Identifiable information, and if so, how that de-identified information may be Used and Disclosed;

vii. That all Disclosures through TEFCA are in accordance with the permitted and required Uses and Disclosures specified in the Common Agreement and applicable U.S. Department of Health and Human Services guidance;

viii. Whether Individually Identifiable information relating to reproductive healthcare services, which as defined in Executive Order 14076[5] means "medical, surgical, counseling, or referral services relating to the human reproductive system, including services relating to pregnancy or the termination of a pregnancy," may be Used and/or Disclosed in accordance with a civil or criminal subpoena, court order, search warrant, or other demand for compulsory disclosure including across state lines in accordance with Applicable Law, even if a service is paid for entirely out-of-pocket by an Individual;

ix. Whether Individually Identifiable information relating to gender affirming care may be Used and/or Disclosed in accordance with a civil or criminal subpoena, court order, search warrant, or other demand for compulsory disclosure including across state lines in accordance with Applicable Law, even if a service is paid for entirely out-of-pocket by an individual;

x. Whether the IAS Provider is subject to the HIPAA Rules, as a matter of law;

xi. Written or electronic notice will be provided to the affected Individual(s) (unless prohibited by Applicable Law) within three (3) business days of the IAS Provider receiving a civil or criminal subpoena, court order, search warrant, or

[4] See Section 4.2 of the SOP below (Consent to Sale).
[5] Executive Order 14076 Protecting Access to Reproductive Healthcare Services available at https://www.govinfo.gov/content/pkg/FR-2022-07-13/pdf/2022-15138.pdf.

other demand for compulsory disclosure in accordance with Applicable Law with respect to the Individually Identifiable information unless such notice is prohibited (e.g., under the Patriot Act). The affected Individual(s) receiving such notice should be afforded the right to object to the production of the Individually Identifiable information or seek a protective order or other appropriate remedy consistent with Applicable Law; and

xii. Written or electronic notice will be provided to the affected Individual(s) (unless prohibited by Applicable Law) within three (3) business days of the IAS Provider making Individually Identifiable information available to law enforcement agencies, including through sale of Individually Identifiable data.

5. Include a statement that the IAS Provider 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 the applicable Framework Agreement.

   a. The statement also must:

      i. State that the IAS Provider uses commercially reasonable efforts to protect Individually Identifiable information from unauthorized or illegal access, modification, Use, or destruction;

      ii. Explain that the IAS Provider encrypts all Individually Identifiable information held by the IAS Provider, both in transit and at rest, regardless of whether such data are TEFCA Information;

      iii. State that the IAS Provider must notify Individuals whose Individually Identifiable information has been or is reasonably believed to have been affected by an IAS Incident[6];

      iv. State that the IAS Provider's obligations under the Privacy and Security Notice will continue for as long as the IAS Provider maintains the Individually Identifiable information;

      v. Give a general description of the privacy and security practices that the IAS Provider requires of third parties that provide any services on behalf of the IAS Provider and with whom the IAS Provider shares Individually Identifiable information in connection with such services.

6. Include information regarding whom the Individual may contact within IAS Provider for further information regarding the Privacy and Security Notice and/or with privacy-related complaints.

   a. The IAS Provider also must:

[6] See details in Section 4.3 of the SOP Below, Content of Notice to Individual of TEFCA Security Incident or Breach of Unencrypted Information.

i. At least within any user-facing application, provide contact information, including telephone number and email address of a person, position, or department within the organization that can respond to questions or complaints; and

ii. Maintain a process for documenting privacy-related complaints, as well as the IAS Provider's response, including the final disposition of such complaints.

7. Include a requirement by IAS Provider 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 of the Individually Identifiable information, other than Disclosures that are required by Applicable Law.

   a. The IAS Provider also must:

      i. Collect the Individual's express written and informed consent, meaning that Individuals are provided with sufficient context at the time consent is requested to understand the consequences of their choices, at the outset of the Individual's first use of the IAS;

      ii. Collect the Individual's express written and informed consent before using Individually Identifiable information in a materially different manner than claimed in the Notice when such information was collected or with any material change in the Notice;

      iii. Include an option to collect/capture/obtain the Individual's express written and informed consent via electronic signature in accordance with Applicable Law. The Electronic Signatures in Global and National Commerce Act (E-Sign Act) (Public Law 106-229) addresses what constitutes a valid electronic signature and provides that a signature may not be denied legal effect because it is in electronic form; and

      iv. Maintain express written and informed consent(s) in a secured auditable log, sufficient to validate and verify the consent.

8. Include information on how the Individual may revoke consent.

   a. The process to revoke consent to the Notice also must:

      i. Not be burdensome to the Individual, with at least an electronic means to revoke consent within any user-facing application(s); and

      ii. Include step-by-step instructions for the Individual to revoke consent:

         1. Step-by-step instructions for revoking consent must be conspicuously displayed in a stand-alone manner on the IAS Provider's website and readily located within user-facing application.

iii. Such revocation will not affect any actions taken by the IAS Provider in reliance on the consent prior to the date of such revocation. Subsequent to the date of such revocation, the Individual will no longer be able to access the IAS Provider services.

9. Include an explanation of the Individual's rights with respect to Individually Identifiable information, including, at a minimum the right of an Individual to:

   i. Require that all of their Individually Identifiable information maintained by the IAS Provider in connection with the IAS 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. Access their Individually Identifiable information maintained by the IAS Provider in connection with the IAS;

   iii. Obtain an export of their Individually Identifiable information in a machine-readable format, including the means to interpret such machine-readable format; and

   iv. Be notified in the event their Individually Identifiable information is reasonably believed to have been affected by an IAS Incident.[7]

   a. The IAS Provider also must:

      i. Describe the choices an Individual has regarding the collection, Use, deletion, and sharing of their Individually Identifiable information, including the Individual's right to opt out of having the IAS Provider Disclose their Individually Identifiable information via TEFCA Exchange;

      ii. Conspicuously display in the Notice clear instructions on how Individuals can exercise those choices, including but not limited to, how to obtain access to or an export of their Individually Identifiable information and the available format(s) in which the Individually Identifiable information can be exported;

      iii. Respect the Individuals' choices by implementing any such choices within a reasonable time period; and

      iv. Inform the Individual if the IAS Provider is reasonably aware of any Applicable Law that would prohibit it from honoring Individuals' request to delete Individually Identifiable information.

10. Include a disclosure of any applicable fees or costs related to IAS including the exercise of any Individual rights.

   a. The disclosure also must:

[7] Notice to the Individual must include the information in Section 3.C of this SOP.

i. Provide clarity around which services will result in fees to an Individual and when fees will be charged to Individuals (e.g., on a monthly or transactional basis), as well as when and how such fees must be paid, with a description of available grace periods and other relevant requirements and/or constraints.

ii. Note the amount of any then-current fees.

11. Include an effective date of the written Notice and an effective date of any subsequent material changes to such Notice.

4.2 Consent to Sale

Notwithstanding anything to the contrary in the Notice, if an IAS Provider intends to sell, or otherwise receive renumeration in exchange for Individually Identifiable information, the IAS Provider must obtain the Individual's prior, express, written consent ("Consent to Sale"). While the IAS Provider may obtain the Consent to Sale contemporaneously with the Individual's consent to the Notice, the Consent to Sale must be conspicuously labeled as such and separate from the consent to the Notice.

4.3 Content of Notice to Individual of TEFCA Security Incident or Breach of Unencrypted Information (IAS Incident)

Notice to an Individual of an IAS Incident in which the Individual's Individually Identifiable information is reasonably believed to have been affected must include, to the extent possible, the following information:

a. A brief description of what happened, including the date of the IAS Incident and the date of its Discovery, if known;

b. A description of the type(s) of Individually Identifiable involved in the IAS 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);

c. Any steps Individuals should take to protect themselves from potential harm resulting from the IAS Incident;

d. A brief description of what the IAS Provider involved is doing to investigate the IAS Incident, to mitigate harm to Individuals, and to protect against any further IAS Incidents; and

e. Contact procedures for Individuals to ask questions or learn additional information related to the IAS 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.

ADDITIONAL RESOURCES

The CARIN Alliance. The CARIN Trust Framework and Code of Conduct available at https://www.carinalliance.com/wp-content/uploads/2020/07/2020_CARIN_Code_of_Conduct_May-2020.pdf

The CARIN Alliance. CARIN UX Guide available at https://carinuxguide.arcwebtech.com/

Centers for Medicare & Medicaid Services (CMS). Toolkit for Making Written Material Clear and Effective (2021) available at Toolkit for Making Written Material Clear and Effective (cms.gov)

State of California, Office of the Attorney General. Making Your Privacy Practices Public: Recommendations on Developing a Meaningful Privacy Policy (2014) available at https://oag.ca.gov/sites/all/files/agweb/pdfs/cybersecurity/making_your_privacy_practices_public.pdf

The Federal Trade Commission (FTC). Mobile Health App Developers: FTC Best Practices (2012) available at https://www.ftc.gov/business-guidance/resources/mobile-health-app-developers-ftc-best-practices

The Federal Trade Commission (FTC). Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Businesses and Policymakers (2012) available at https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf

The Federal Trade Commission (FTC). Complying with COPPA: Frequently Asked Questions (2020) available at https://www.ftc.gov/business-guidance/resources/complying-coppa-frequently-asked-questions#A.%20General%20Questions

National Telecommunications and Information Administration. Short Form Notice Code of Conduct to Promote Transparency in Mobile App Practices (2013) available at https://www.ntia.doc.gov/files/ntia/publications/july_25_code_draft.pdf

U.S. Department of Health and Human Services. Examining Oversight of the Privacy & Security of Health Data Collected by Entities Not Regulated by HIPAA (2016) available at https://www.healthit.gov/sites/default/files/non-covered_entities_report_june_17_2016.pdf.

U.S. Department of Health and Human Services, Office for Civil Rights (OCR). Model Notices of Privacy Practices Webpage (Last reviewed 2013) available at https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/model-notices-privacy-practices/index.html

U.S. Department of Health and Human Services, Office for Civil Rights (OCR). FAQ Regarding Fees (2020) available at https://www.hhs.gov/hipaa/for-professionals/faq/2024/may-a-covered-entity-charge-individuals-a-fee/index.html

U.S. Department of Health and Human Services, Office of the National Coordinator for Health Information Technology (ONC). Model Privacy Notice (2018) available at https://www.healthit.gov/topic/privacy-security-and-hipaa/model-privacy-notice-mpn

U.S. Department of Health and Human Services, Office of the National Coordinator for Health Information Technology (ONC). Information Blocking FAQs available at https://www.healthit.gov/curesrule/resources/information-blocking-faqs

U.S. Department of Health and Human Services, National Committee on Vital and Health Statistics. Health Information Privacy Beyond HIPAA: A Framework for Use and Protection – A Report for Policy Makers (2019) available at https://ncvhs.hhs.gov/wp-content/uploads/2019/07/Report-Framework-for-Health-Information-Privacy.pdf

United States Government. Plain Language Website available at www.plainlanguage.gov

VERSION HISTORY

Version	Revision Date	Section #(s) of Update
Standard Operating Procedure (SOP): Individual Access Services (IAS) Provider Privacy and Security Notice and Practices Version 1.0	Released 12/11/2023	N/A
Standard Operating Procedure (SOP): Individual Access Service (IAS) Provider Requirements Version 2.0	Released 1/19/24	All sections