ONC
TEFCA
RECOGNIZED
COORDINATING
ENTITY

Standard Operating Procedure (SOP): Individual Access Services (IAS) Provider Privacy and Security Notice and Practices

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

1. Common Agreement References

Capitalized terms used below without definitions shall have the respective meanings assigned to such terms in the Common Agreement and the QHIN Technical Framework.

CA Section 1: Defined Terms

- Individual
- Individual Access Services (IAS)
- Individually Identifiable
- IAS Provider
- TEFCA Information

CA Section 10.3: Written Privacy and Security Notice and Individual Consent

CA Section 10.4: Individual Rights

CA Section 10.5.1: Scope of Security Requirements

CA Section 10.5.2: Encryption

CA Section 10.6: Survival for IAS Providers

CA Section 11.1: Compliance with the HIPAA Privacy Rule

2. Purpose

The Trusted Exchange Framework and Common Agreement (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 participate in TEFCA exchange. Among other things, IAS Providers are required to obtain the Individual's express written consent in connection with Individual Access Services, including agreement and acknowledgment to the IAS Provider's written Privacy and Security Notice

(Notice) that describes the privacy and security practices used to safeguard Individually Identifiable information.[1]

This SOP details the requirements and specifications for IAS Providers to follow in implementing such Notice. This includes both requirements regarding the content of a Privacy and Security Notice and the required corresponding practices of an IAS Provider related to those Notice requirements. Requirements that fall under the IAS Exchange Purpose Implementation SOP, which is focused on identity proofing requirements, are out of scope for this SOP.

The U.S. Department of Health and Human Services has identified that the lack of appropriate and understandable privacy policies and notices is an issue for entities not regulated by HIPAA.[2] The Federal Trade Commission (FTC) has called for improved data practice transparency, encouraging privacy policy statements that are "clearer, shorter, and more standardized to enable better comprehension and comparison of privacy practices."[3]

Services that offer an Individual access to their Individually Identifiable information have an important role to play in developing policies that are clear and understandable to users. As such, IAS Providers must satisfy the requirements herein in order to promote transparency in how Individually Identifiable information is protected and safeguarded. By upholding these standards, IAS Providers can improve how Individuals understand the selected IAS Providers' information privacy practices and security protections, allowing Individuals to make informed decisions about who to entrust with their information.

3. PROCEDURE

Common Agreement Section 10.3.1: Written Privacy and Security Notice and Individual Consent

A. If Signatory offers Individual Access Services (IAS), it must develop and make publicly available a written privacy and security notice (the "Notice"). If Signatory is a Covered Entity, then a Notice of Privacy Practices that meets the requirements of 45 CFR § 164.520 **and** meets the requirement of this SOP can satisfy the Privacy and Security Notice requirements. Nothing in this SOP reduces a Covered Entity's obligations under the HIPAA Rules.

[1] Nothing in this SOP alters a Covered Entity's obligations under the HIPAA Rules.
[2] 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.
[3] 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 Privacy and Security Notice must:

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 services 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:

         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 services from Signatory;

   a. The IAS Provider also must:

      i. Provide the Notice in a timely manner to allow 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[4];

      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[5]; and

      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 the Individual's TEFCA Information may be accessed, exchanged, Used, and/or Disclosed by Signatory or by other persons or entities to whom/which Signatory Discloses or provides access to the information, including whether the Individual's TEFCA Information may be sold at any time (including the future)

   a. The statement also must clearly explain:

      i. That TEFCA 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 TEFCA Information may be further accessed by, exchanged with, Used by and/or Disclosed to third parties;

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

[4] https://www.plainlanguage.gov/guidelines/
[5] https://www.hhs.gov/guidance/sites/default/files/hhs-guidance-documents//cy2021_translated_model_materials_requirements_and_language_data_analysis_methodology.pdf

iv. The period of time for which the IAS Provider will retain the TEFCA Information;

v. The specific purpose for any Use of TEFCA Information, provided such use must be consistent with 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[6]). Any direct Disclosures to the Individual do not require such an explanation in the Notice;

vi. Whether the IAS Provider will de-identify TEFCA 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 TEFCA Information relating to reproductive healthcare services, which as defined in Executive Order 140767 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 TEFCA 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;

[6] See Section 3B of the SOP below (Consent to Sale)
[7] https://www.govinfo.gov/content/pkg/FR-2022-07-13/pdf/2022-15138.pdf

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 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 TEFCA 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 TEFCA Information available to law enforcement agencies, including through sale of individually identifiable data.

5. Include a statement that Signatory 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 Common Agreement;

a. The statement also must:

i. State that the IAS Provider uses commercially reasonable efforts to protect all 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, in accordance with Section 10.5.2 of the Common Agreement;

iii. State that the IAS Provider must notify Individuals whose TEFCA Information has been or is reasonably believed to have been affected by a TEFCA Security Incident involving the IAS Provider, in accordance with Section 10.5.3 of the Common Agreement;

iv. State that the IAS Provider's obligations under the Privacy and Security Notice will continue for as long as the TEFCA Information survives in accordance with Section 10.6 of the Common Agreement; and

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 Signatory for further information regarding the Privacy and Security Notice and/or with privacy-related complaints;

   a. The IAS Provider also must:

      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 Signatory 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 TEFCA 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 TEFCA Information in a materially different manner than claimed in the Notice when such information was collected or with any material change in the Notice, as required in Section 10.3.2 of the Common Agreement;

      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 the user-facing application; 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, including, at a minimum, the rights set forth in Section 10.4 of the Common Agreement;

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 revoke their consent to 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 rights under Section 10.4 of the Common Agreement; and

a. The disclosure also must:

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; and

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

11. Include an effective date.

B. 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 TEFCA 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. Additional Resources

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: https://www.cms.gov/outreach-and-education/outreach/writtenmaterialstoolkit/downloads/toolkitpart11.pdf

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