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

DRAFT FOR PUBLIC FEEDBACK

RELEASED 6.21.22 WITH FEEDBACK DUE BY 7.21.22

Applicability: IAS Providers

1 COMMON AGREEMENT REFERENCES

CA Section 10.3:

Written Privacy and Security Notice and Individual Consent **(Required Flow-Downs)**.

10.3.1 If Signatory 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 prior to the Individual's use/receipt of services from Signatory;

(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 TI 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 TI may be sold at any time (including the future);

(v) 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 this Common Agreement;

(vi) 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;

(vii) 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 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 10.4, below;

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

(xi) Include an effective date.

The implementation of such Privacy and Security Notice requirements shall be set forth in the IAS SOP. 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 10.3.1(iv) above can satisfy the Privacy and Security Notice requirements. Nothing in this Section 10.3 reduces a Covered Entity's obligations under the HIPAA Rules.

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

2 PURPOSE

This SOP details the requirements and standards for IAS Providers to follow in implementing a Privacy and Security Notice.[1] 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.

3 STANDARD

The Trusted Exchange Framework and Common Agreement (TEFCA) enables Individuals to access their Individually Identifiable information via an IAS Provider's app, 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.

The 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

[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.

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.

4 PROCEDURE

IAS Providers are required to develop and make publicly available a written Privacy and Security Notice ("Notice") that provides a clear explanation of the privacy practices and security protections of the IAS Provider with respect to the Individual's Individually Identifiable information. IAS Providers must implement the Notice using the following standards.

The Notice must:

1. Common Agreement Section 10.3.1.(i): "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

[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.

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*[4] 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 burden is on the IAS Provider to prove the change was immaterial.

2. Common Agreement Section 10.3.1.(ii): "Be shared with an Individual prior to the Individual's use/receipt of services from [the IAS Provider]"

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. Common Agreement Section 10.3.1.(iii): "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. Use plain, straightforward language and avoid using legal jargon[5];

ii. Use short sentences and the active grammatical voice;

iii. Keep language, at most, at a 6th grade reading level;

iv. Use titles and headers to emphasize key parts of the policy;

[4] See FTC Policy Statement on Deception (1983) for clarification on the term "material." A change will be considered "material" if the act or practice is likely to affect the consumer's conduct or decision with regard to a product or service. The policy statement is accessible from FTC's website or here: https://www.ftc.gov/system/files/documents/public_statements/410531/831014deceptionstmt.pdf

[5] The IAS Provider should evaluate the notice against the latest version of the Federal Plain Language Guidelines. https://www.plainlanguage.gov/guidelines/

1. At least, include the words “Privacy and Security Notice” in the Notice title

v. Provide the Notice in at least English, Spanish, and any other language that reflects the IAS Provider’s customer base; and

vi. Use a format that makes the policy readable, including on smaller screens such as a mobile device:

1. Consider a format that highlights the most relevant privacy and security issues or allows users to show and hide the information one section at a time; and

2. Use graphics or icons to help readers easily recognize privacy and security practices and settings.

4. Common Agreement Section 10.3.1.(iv): “Include a statement regarding whether and how the Individual’s TI may be accessed, exchanged, Used, and/or Disclosed by [the IAS Provider] or by other persons or entities to whom/which [the IAS Provider] Discloses or provides access to the information, including whether the Individual’s TI may be sold at any time (including the future)”

a. The statement also must clearly state the following:

i. Explain if Individually Identifiable information that the IAS Provider reasonably believes to be TI may be further accessed by, exchanged with, Used by and/or Disclosed to third parties;

ii. Explain the specific purpose for any Use of Individually Identifiable information the IAS Provider reasonably believes to be TI. 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, is being sold downstream, or is being given away in exchange for something of value now or in the future, such detail must be made clear to the user). Any direct Disclosures to the Individual do not require such an explanation in the Notice;

iii. Explain whether the IAS Provider will de-identify TI, and if so, how that de-identified information may be Used and Disclosed;

iv. Describe the types of persons/entities to which the Individually Identifiable information the IAS Provider reasonably believes to be TI may be further Disclosed, if any; and

v. Provide the period of time for which the IAS Provider will retain the Individually Identifiable information the IAS Provider reasonably believes is TI.

5. Common Agreement Section 10.3.1.(v): "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 Section 10 of [the] Common Agreement"

    a. The statement also must:

        i. State that the IAS Provider uses commercially reasonable efforts to protect the Individual's 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 TI;

        iii. State that the IAS Provider must notify Individuals whose TI has been or is reasonably believed to have been affected by a TEFCA Security Incident involving the IAS Provider;

        iv. State the minimum provisions with minimum time periods, as required by the flow-down provisions in Common Agreement Section 10.6, that continue even after expiration or termination of the IAS Provider's contractual obligations whereby the data was obtained. For purposes of complying with Section 10.6.1(ii) of the Common Agreement, or the parallel required flow down provisions of the applicable Framework Agreement(s), while the Individual is receiving IAS and during the required survival period following termination of those services, the IAS provider must comply with Section 7(a)(ii) of this SOP;

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

6. Common Agreement Section 10.3.1.(vi): "Include information regarding whom the Individual may contact within [the IAS Provider] 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.

7. Common Agreement Section 10.3.1.(vii): "Include a requirement by [the 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 (including sale) of the Individual's TI, other than Disclosures that are required by Applicable Law"

a. The IAS Provider also must:

i. Collect the individual's express written consent at the outset of the Individual's first use of the IAS;

ii. Collect the individual's express written consent before using TI in a materially different manner than claimed in the Notice when TI was collected; and

iii. Include an option to collect/capture/obtain the Individual's express written 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.

8. Common Agreement Section 10.3.1.(viii): "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 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. Common Agreement Section 10.3.1.(ix): "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 a consumer has regarding the collection, Use, deletion, and sharing of their Individually Identifiable information;

        ii. Conspicuously display in the Notice clear instructions on how Individuals can exercise those choices, including but not limited to, how to obtain 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, to the extent applicable, 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. Common Agreement Section 10.3.1.(x): "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"

    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 description of available grace periods and other relevant requirements and/or constraints; and

        ii. Note the amount of any then current fees.

11. Common Agreement Section 10.3.1.(xi): "Include an effective date" [of the written Notice and an effective date of any subsequent material changes to such Notice]

5 ADDITIONAL RESOURCES

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

2. Centers for Medicare & Medicaid Services (CMS). Toolkit for Making Written Material Clear and Effective (2021), available at https://www.cms.gov/outreachandeducation/outreach/writtenmaterialstoolkit?redirect=/writtenmaterialstoolkit/

3. 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

4. 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

5. 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

6. 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

7. 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.

8. 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

9. 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

10. 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

11. 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

12. 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

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

This program is supported by the Office of the National Coordinator for Health Information Technology (ONC) of the U.S. Department of Health and Human Services (HHS) under grant number 90AX0026, Trusted Exchange Framework and Common Agreement - Recognized Coordinating Entity (RCE) Cooperative Agreement Program, in the amount of $2,919,000 with 100 percent funded by ONC/HHS. This information or content and conclusions are those of the author and should not be construed as the official position or policy of, nor should any endorsements be inferred by ONC, HHS or the U.S. Government.