# Security and Privacy Questionnaire

## Purpose of this Document

Individuals who use Personal Health Applications (PHAs) to collect and store their medical records should be aware of what policies and procedures each PHA has in place to protect and secure their data.

The CARIN Alliance is an independent third party committed to advancing the ability for consumers and their authorized caregivers to easily get, use, and share their digital health information when, where, and how they want to achieve their goals. To facilitate this vision, they have developed the CARIN Alliance Trust Framework and Code of Conduct to provide guidelines and set expectations for PHA providers' data practices and policies.

Using the Trust Framework and Code of Conduct, the CARIN Alliance developed a questionnaire intended to highlight the steps a PHA has taken to ensure security and privacy. The following pages include answers to each question, with a summary of each PHAs answers at the top so that individuals can assess each PHA and make an informed decision on which to entrust with their medical records.

## Personal Health Application

**Name of PHA:** ***OtisHealth***

**Name of PHA Provider:** ***OtisHealth***

# Security and Privacy Summary

The *OtisHealth* PHA:

- The *OtisHealth* is not a HIPAA covered entity or a HIPAA business associate
- *OtisHealth* follows the data practices outlined in the CARIN Alliance Trust Framework and Code of Conduct
- *OtisHealth* is not registered on the CARIN Alliance's MyHealthApplication.com.
- *OtisHealth* has a publicly accessible link to the PHA's Privacy Policy. the privacy policy:
    - covers collection, use and disclosure of Personal Data (as defined in the CARIN Alliance Code of Conduct)
    - covers collection, use and disclosure of De-identified Information
    - is clear about what happens to Data when Consent is reaffirmed or withdrawn.
    - is clear about what happens to Data if the PHA Provider has a change in ownership or the PHA Provider (or PHA Developer, if different from the PHA Provider) goes out of business.
    - is clear about the scope of information collected by the PHA
    - is clear about the scope of permitted uses of Personal Data.
    - is clear about the scope of permitted Disclosures, when the PHA will collect an informed, proactive Consent before sharing a user's Data with third parties and when Disclosures are permitted without an informed, proactive Consent (for example, as required by law or in connection with the business transfer).
    - requires the PHA to collect a separate Consent if the purpose of Disclosure is to facilitate the marketing of goods or services to the individual.
- *OtisHealth* provides updates when Privacy Policies have changed, and provides individuals with the option to reaffirm Consent or to withdraw Consent
- *OtisHealth* only collects Personal Data through external data connections with users' consent
- *OtisHealth* only collects Personal Data with users' Consent, and will continue to do so until the User revokes Consent.
- *OtisHealth* prohibits Uses of Personal Data and De-identified Information except with Consent from the individual

- *OtisHealth* does not collect a separate Consent before marketing third party goods or services to an individual
- *OtisHealth*:
    - supports the right of users to access their Data.
    - supports the right of users to easily change their Consent options.
    - supports the right of users to close their account and delete their Data and is clear about situations when data deletion may not be feasible.
    - supports the right of users to send Personal Data to the destination of their choice.
- To ensure data security, *OtisHealth*:
    - protects identifiable health information by implementing security safeguards including encryption of data in transit and at rest and internal accountability measures such as access controls and audit logs.
    - complies with applicable breach notification laws.
    - uses provider portal credentials (compliant with SMART on FHIR/Open ID Connect standards) or a digital identity credential that meets NIST 800-63 identity assurance level 2.
    - prohibit re-identification of De-Identified/Anonymized/Pseudonymized Data
- *OtisHealth* complies with all applicable federal and state laws and regularly trains their workforce on compliance with the data practices covered by the CARIN Code of Conduct.
- In the last 12 months, *OtisHealth* has not been reviewed by an independent assessment organization for compliance between its Privacy Policy and AICPA Privacy Principles and has not received SOC-2 certification.
- In the last 12 months, *OtisHealth* has not been certified for compliance with the HITRUST CSF.

# Complete Questionnaire

Read the entire questionnaire, as completed by *OtisHealth*, below:

1. Is the PHA Provider

☐ a HIPAA covered entity

☐ a HIPAA business associate

✔ not a HIPAA covered entity or a HIPAA business associate

2. Do the PHA's data practices follow the CARIN Alliance Trust Framework and Code of Conduct?

✔ Yes

☐ No

☐ Not Sure (Complete Questions 3 – 10, Below)

3. Has the PHA been registered on CARIN Alliance's MyHealthApplication.com?

☐ Yes

✔ No

4. Transparency –

a. The PHA Provider includes a publicly accessible link to the PHA's Privacy Policy on its website and through the PHA:

✔ Yes

☐ No

b. The Privacy Policy covers collection, use and disclosure of Personal Data (as defined in the CARIN Alliance Code of Conduct):

✔ Yes

☐ No

c. The Privacy Policy covers collection, use and disclosure of De-identified Information (as defined in the CARIN Alliance Code of Conduct):

✔ Yes

☐ No

d. The PHA Provider provides updates when Privacy Policies have changed, and

provides individuals with the option to reaffirm Consent or to withdraw Consent

✔ Yes

☐ No

e. The Privacy Policy is clear about what happens to Data (as defined in the CARIN Alliance Code of Conduct) when Consent is reaffirmed or withdrawn.

✔ Yes

☐ No

f. The Privacy Policy is clear about what happens to Data (as defined in the CARIN Alliance Code of Conduct) if the PHA Provider has a change in ownership or the PHA Provider (or PHA Developer, if different from the PHA Provider) goes out of business.

✔ Yes

☐ No

5. Questions about Data Collection

a. The Privacy Policy is clear about the scope of information collected by the PHA.

✔Yes

☐ No

b. The PHA only collects Personal Data through external data connections with users' consent (as outlined in the CARIN Alliance Code of Conduct).

✔ Yes

☐ No

c. The PHA only collects Personal Data with users' Consent (as outlined in the CARIN Alliance Code of Conduct).

✔ Yes

☐ No

d. After collecting Personal Data from an external source, the PHA –

☐ Continues to collect new Personal Data as it becomes available until the user revokes Consent

✔ Requires Consent each time before collecting additional Personal Data from that source

6. Questions about Data Uses (as outlined in the CARIN Alliance Code of Conduct) by the PHA

a. The Privacy Policy is clear about the scope of permitted uses of Personal Data.

✔ Yes

☐ No

b. The PHA Developer (if different from the PHA Provider) and all other third-party service providers are contractually obligated to follow the Privacy Policy

✔ Yes

☐ No

c. The PHA Provider prohibits Uses of Personal Data and De-identified Information except with Consent from the individual

✔ Yes

☐ No

d. The Organization collects a separate Consent before marketing third party goods or services to an individual

☐ Yes

✔ No

7. Questions about Disclosures (as outlined in the CARIN Alliance Code of Conduct) of Data to Third Parties

a. The Privacy Policy is clear about the scope of permitted Disclosures, when the PHA will collect an informed, proactive Consent before sharing a user's Data with third parties and when Disclosures are permitted without an informed, proactive Consent (for example, as required by law or in connection with the business transfer).

✔Yes

☐ No

b. The Privacy Policy requires the PHA to collect a separate Consent if the purpose of Disclosure is to facilitate the marketing of goods or services to the individual.

✔ Yes

☐ No

8. Questions about Individual Rights

a. The PHA supports the right of users to access their Data.

✔ Yes

☐ No

b. The PHA supports the right of users to easily change their Consent options.

✔ Yes

☐ No

c. The PHA supports the right of users to close their account and delete their Data and is clear about situations when data deletion may not be feasible.

✔ Yes

☐ No

d. The PHA supports the right of users to send Personal Data to the destination of their choice.

✔ Yes

☐ No

9. Questions about Data Security

a. The PHA Provider and PHA Developer (if different from the PHA Provider) protects identifiable health information by implementing security safeguards including encryption of data in transit and at rest and internal accountability measures such as access controls and audit logs.

✔ Yes

☐ No

b. The Organization and App Developer (if different from the Organization) comply with applicable breach notification laws.

✔ Yes

☐ No

c. The PHA Provider and PHA Developer (if different from the PHA Provider) use provider portal credentials (compliant with SMART on FHIR/Open ID Connect standards) or a digital identity credential that meets NIST 800-63 identity assurance level 2.

✔ Yes

☐ No

d. The PHA Provider and PHA Developer (if different from the PHA Provider) prohibit re-identification of De-Identified/Anonymized/Pseudonymized Data (as defined in the CARIN Alliance Code of Conduct).

✔ Yes

☐ No

10. Question about Accountability

a. The PHA Provider and PHA Developer (if different from the PHA Provider) comply with all applicable federal and state laws.

✔ Yes

☐ No

b. The PHA Provider and PHA Developer (if different from the PHA Provider) regularly train their workforces on compliance with the data practices covered by the CARIN Code of Conduct.

✔ Yes

☐ No

11. Questions About Certifications

a. In the last 12 months, the PHA's data practices have been reviewed by an independent assessment organization for compliance with the PHA's Privacy Policy and AICPA Privacy Principles and is documented by a written SOC-2 certification report.

☐ Yes

✔ No

b. In the last 12 months, the PHA's data practices have been certified by an independent assessment organization for compliance with the HITRUST CSF.

☐Yes

✔ No