Request for Proposals:

Consumer Privacy Framework for Health Data – Self-Regulatory Program Implementation and Organizational Home

Released January 2022

The Consumer Privacy Framework for Health Data was developed by the Center for Democracy & Technology (CDT) and Executives for Health Innovation (EHI) and funded by the Robert Wood Johnson.

BACKGROUND

Every day the line between “health data” and “consumer data” is further blurred. It used to be that health data was held near-exclusively by the healthcare system – hospitals, doctors, clinics, and health insurers. But with the explosive proliferation of digital technologies – first the internet, and later consumer-facing apps, connected fitness and health tracking devices, and web-based platforms – an ever-increasing amount of health data is generated by consumers themselves, and both held and used by companies that are not bound by the obligations of the Health Insurance Portability and Accountability Act (HIPAA), the nation’s primary health privacy law.

These vast troves of valuable, sensitive health data are currently woefully under-protected by our federal legal and regulatory regime. Since 1996, *only* information collected by hospitals, insurers, doctors and clinics is covered by HIPAA and its subsequently implemented Privacy and Security rules. Most other health data stored digitally remains largely under-protected and under-regulated.

THE CONSUMER PRIVACY FRAMEWORK FOR HEALTH DATA

It was in this context of outdated privacy models that Executives for Health Innovation (EHI, formerly the eHealth Initiative) and the Center for Democracy & Technology (CDT) developed the *Consumer Privacy Framework for Health Data (*hereinafter “*the Framework*”), made possible by the generous support of the Robert Wood Johnson Foundation (RWJF).[1] In an effort to address the current gaps in legal protections, *the Framework* outlines how all types of health-related data should be used, accessed, and disclosed. Historically, many privacy models have placed too much emphasis on individuals consenting to the use of and access to their health data and company notifications. These outdated privacy models have failed to protect consumers and meaningfully inform them about how their data might be or is actually used.

The Framework involves a detailed set of data use limits; covers all information that can be used to make inferences or judgments about a person’s physical or mental health by virtue of a broad definition of “consumer health information;” and applies to all non-HIPAA-covered entities that collect, disclose, or use consumer health information, regardless of the size or business model of the covered entity.

[1] Proposed Consumer Privacy Framework for Health Data. (2021, February). Center for Democracy & Technology. Executives for Health Innovation. Report. Hereinafter, “Consumer Privacy Framework.” https://www.ehidc.org/sites/default/files/eHIDCT_Consumer_Privacy_Framework.pdf

The Framework was developed through a process involving the input of some 60 organizations from across the healthcare spectrum – technology companies, digital health companies, provider associations, payers, academia, consumer and patient groups, and privacy and civil liberties organizations – who made up an advisory Steering Committee.

ACCOUNTABILITY PROGRAM

A central goal of *the Framework* is to advance a proposal with more significant impact on shoring up consumer privacy protections than existing laws, codes of conduct, or sets of best practices. Inherent in that goal is meaningful accountability for misuse of consumer health data by non-HIPAA-covered entities. Although it appears unlikely that new comprehensive federal privacy legislation is on the near-term horizon, continued and recent enforcement actions show that harmful data practices surrounding consumer health data show no signs of slowing. While we wait for federal action, is a critical for the private sector to implement data use accountability standards based on the those set forth in *the Framework*. As such, *the Framework* proposes that the data use rule-set, and entities' adherence to it, be governed by a new independent private-sector self-regulatory program.

Self-regulation has been successfully employed in other contexts and industries, particularly finance and advertising, and this is an opportunity to apply lessons learned from those programs to health tech.

A governance body tasked with managing member companies, providing onboarding and education, conducting regular audits, and developing corrective action plans or further disciplinary actions – including direct referral to the Federal Trade Commission (FTC) for non-compliance, would provide real, consequential accountability in the absence of federal legal obligations. Identifying this body is the primary purpose of this Request for Proposal (RFP).

PURPOSE

Through this RFP, EHI will select an organization to house, implement and run a self-regulatory program to govern member companies' compliance with the data-use standards contained within the Framework. Once an organization is chosen, EHI will partner with it to explore funding opportunities to provide seed money for the development and launch of the program.

The primary purpose of this project is to make the proposed self-regulatory program a reality by staffing the accountability infrastructure, recruiting member companies, developing the technological certification expertise, creating a financially sustainable model, and producing a consumer-facing and user-friendly website.

WHO CAN APPLY

We encourage proposals from organizations with experience initiating, implementing and managing certification and self-regulatory programs, preferably within or related to the health and/or technology sectors. EHI will provide project management support, assistance with publicity and member recruitment, and overall amplification of the effort.

KEY DATES

FRIDAY, FEBRUARY 11, 2022 | 5:00 PM EST

APPLICATIONS DUE TO ALICE@EHIDC.ORG

FRIDAY, FEBRUARY 25, 2022

SELECTION ANNOUNCED

SELECTION CRITERIA

All proposals will be screened for eligibility and then assessed by a committee composed of EHI staff, a selection of EHI board members, and expert external reviewers.

Selection will be based on the applicant's:

- Experience running a self-regulatory program and/or certification program;
- Familiarity with health data privacy and security;
- Relationship with the technology industry, and health-tech in particular;
- Plan to recruit members to this program;
- Proposed budget, including a plan to make the program financially sustainable;
- Staffing plan, including the requisite technological capabilities and expertise;
- Plans to create a transparent, consumer-facing program; and
- Relationships with and planned engagement of relevant federal regulatory authorities.

HOW TO APPLY

Applicants will submit a full proposal, budget, budget narrative, and organizational documents for review.

The proposal will consist of responses to specific questions contained in the attached application form that are designed to provide reviewers with information necessary to assess the extent to which they meet the criteria listed above.

All proposals and supporting documents must be submitted electronically by e-mailing the materials to alice@ehidc.org by **Friday, February 11, 2022, at 5:00 PM EST.**

STAFFING

Applicants should consider a staffing structure that reflects a realistic estimate of the time it will take to stand up a nascent self-regulatory program. This includes the requisite technological expertise to both understand *the Framework's* rule-set and evaluate companies' adherence to it; the ability to conduct member company education and on-boarding, regular assessments, and audits; the implementation of corrective action plans when necessary; maintenance of a website that allows for easy promotion of member companies, detailed information about the program and its goals, and a clear, simple ability for consumer complaint-submission; and effective engagement of decision-makers.