Proposed Consumer Privacy Framework for Health Data

Draft for Public Feedback

August 26, 2020

eHealth Initiative

Center for Democracy and Technology

Table of Contents

Background

Health data — or data used for health-related purposes — is not regulated by a single national privacy framework. Since 1996, the Health Insurance Portability and Accountability Act (HIPAA) has governed the use and disclosure of certain health information held by certain entities like doctors and insurance companies. However, with the rise of wearable devices, health and wellness apps, online services, and the Internet of Things (IoT), extraordinary amounts of information reflecting mental and physical wellbeing are created and held by entities who are not bound by HIPAA obligations. This issue has only gained importance in the last several months, as new regulations will also be moving HIPAA-covered medical records into this commercially-facing and unregulated space. The novel coronavirus, too, has thrust the issue of patient data privacy to the forefront, as efforts to trace and combat the spread of the virus has brought with it the relaxation of some federal privacy protections, as well as increased data collection and use.

Project Goals and Status

With funding from the Robert Wood Johnson Foundation, the eHealth Initiative (eHI) and the Center for Democracy & Technology (CDT) have been collaborating on a Consumer Privacy Framework for Health Data, with invaluable engagement and help from a Steering Committee of leaders from healthcare providers, technology companies, academia, and organizations advocating for privacy, consumer, and civil rights. Two workgroups – focused on the Framework's Substance and Structure – have developed detailed use, access, and disclosure principles and controls for health data designed to address the gaps in legal protections for health data outside HIPAA's coverage, along with a draft self-regulatory model to support enforcement of such standards. The standards' emphasis is on transparency, accountability, and the limitation on health data collection, disclosure, and use. Importantly, the standards:

(1) move beyond outdated notice and consent models,

(2) cover all health information, and

(3) cover all entities that use, disclose or collect consumer health information, regardless of the size or business model of the covered entity.

This proposal is not designed to be a replacement for necessary comprehensive data privacy legislation. Given that Congressional action to pass such a law is likely some time away, this effort is designed to build consensus on best practices and to do what we can now, in the interim, to shore up protections for non-HIPAA covered health data.

Value of this Proposal

Consumers. This model raises the bar for consumer privacy. Some existing best practices or voluntary frameworks define health information quite narrowly, and do not cover all of the data that reflects mental or physical wellbeing or health. Many best practices are also often targeted at a specific type of app or service instead of all entities that collect and use health data. Our comprehensive proposal closes these gaps in coverage.

Substantively, our draft goes beyond outdated models that revolve primarily around notice and consent. While such laws or frameworks may have made sense in decades past, people can no longer make informed and timely decisions about all the different websites, apps, and devices they use everyday. By putting clear restrictions on the collection, use, and sharing of data, the draft shifts the burden of privacy risk off of users.

Finally, because our model borrows the best concepts from Europe and California, users will benefit from these heightened protections even if their local laws have not been updated with more modern data privacy protections.

Companies and organizations that collect health information. Entities that elect to participate and adopt the framework will also benefit. First, they will stay ahead of the regulatory curve. By making pro-privacy decisions now, they will avoid having to make product changes that could be more expensive, time consuming, or complicated in response to future regulation.

Second, while entities will be able to develop and offer the product a consumer requests, they will be deterred from collecting and using health data they do not actually need. This should reduce both legal and reputational risks in a world where the public and enforcement agencies expect more from companies that handle data.

Finally, this model has the potential to provide some compliance certainty for members. By adopting more forward-looking privacy practices, companies and organizations will avoid practices in the gray or evolving areas of existing laws. Compliance with these standards would provide some assurance that participants have met various federal and state requirements.

Regulators and oversight bodies. Congress, the Federal Trade Commission, and their state-level counterparts will benefit from the commitment to publicly-available rules. It will allow them to enforce these promises, which will be more explicit than many existing privacy policies. Instead of engaging in complicated investigations and balancing tests, these entities will be able to measure compliance more easily.

Additionally, if the self-regulatory model includes third party audits or enforcement, there will be instances to investigate and prosecute, allowing these agencies to focus their resources on bad actors who would not otherwise be compelled to act in pro-privacy ways.

Proposed Substance of Framework and Policy Rationale

For any follow up questions, kindly contact Andy Crawford at CDT (acrawford@cdt.org)

Definitions

1. **Affirmative Express Consent** -
    a. In General - The term "affirmative express consent" means an affirmative act by a consumer that clearly communicates the consumer's authorization for an act or practice, in response to a specific request that -
        i. Is provided to the consumer in a clear and conspicuous disclosure that is separate from other options or acceptance of general terms; and
        ii. Includes a description of each act or practice for which the consumer's consent is sought and;
            1. Is written concisely and in easy-to-understand language; and
            2. Includes a prominent heading that would enable a reasonable consumer to identify and understand the act or practice.
    b. Express Consent Required - Affirmative express consent shall not be inferred from the inaction of a consumer or the consumer's continued use of a service or product.
    c. Voluntary - Affirmative express consent shall be freely given and nonconditioned.

The data covered by this framework is inherently sensitive and it is crucial that consent for its collection, use, and sharing be meaningful. It has been repeatedly documented that hiding terms in a privacy policy does not meet this standard. To that end, this definition requires the clear and thorough presentation of information to users and clarifies that consent cannot be inferred from consumer inaction. Moreover, consumer consent must be voluntary and cannot be conditioned. This approach is also consistent with the FTC's approach, other frameworks, and bipartisan constructions of affirmative express consent introduced during the 116th Congress, including comprehensive privacy legislation and legislation targeting consumer health information.

2. **Aggregated Data** - The term "aggregated data" means consumer health information that relates to a group or category of consumers but cannot reasonably be used to infer information about, or otherwise be linked to, an individual, a household, or a device used by an individual or household. A participating entity wishing to use aggregated consumer health information shall -
    a. Take reasonable measures to safeguard the aggregated consumer health information from reidentification;
    b. Publicly commit in a conspicuous manner not to attempt to reidentify or associate the aggregated consumer health information with any consumer or device linked or reasonably linkable to a consumer;

c. Collect, disclose, or use the aggregated consumer health information for research purposes only; and
d. Contractually require the same commitment for all transfers of the aggregated consumer health information.

This framework recognizes that properly aggregated data should pose fewer privacy risks to individuals and communities. As a result of that reduced privacy risk, this framework permits certain uses of aggregated data because it can achieve positive societal purposes with fewer individualized risks, in ways that identifiable data sets cannot. Importantly, aggregation is not a silver bullet in protecting individual privacy. This framework includes requirements to limit the use of aggregated data to research purposes.

3. **Consumer** - The term "consumer" means an individual.

4. **Consumer Health Information** - The term "consumer health information" means -
    a. Any information, recorded in any form or medium, that—
        i. Is created or received by an entity; and
            1. Relates to or is used to determine, predict, or estimate the past, present, or future physical or mental health condition of an individual; or
            2. Relates to the provision of health care to an individual, and
    b. The following data sets regardless of the purpose or outcome of the collection, disclosure, or use—
        i. Data that reflects racial and ethnic origin;
        ii. Genetic data;
        iii. Biometric data;
        iv. Data that reflects reproductive health;
        v. Data that reflects sexual orientation;
        vi. Data that reflects disability;[1]
        vii. Data that reflects sensitive disease conditions; and
        viii. Data that reflects substance abuse.

This definition intentionally rejects previous notions of "health data" that are limited to the direct provision of health services by a professional. It also avoids the approach taken by some other voluntary frameworks that create a list of health conditions that qualify for protection. This definition instead focuses on the nature of the information and how it is used. It recognizes that all data can be "health data" if it is used for those purposes, even if it appears unrelated on its face. To that end, subsection (a) covers all data that a participant collects, shares, or uses for health purposes. Subsection (b) declares that certain sensitive health topics shall always be subject to the framework, regardless of the context of their use. This framework does not include an exception for employee data.

[1] As defined under that Americans with Disabilities Act of 1990.

A purpose- and use-based approach to this definition has several benefits. First, it benefits consumers by raising the bar for all the data that is used to impact their health and wellness. Modern data use is complex, opaque, and instantaneous. Trying to delineate distinct data sets as worthy of coverage and others as not no longer makes sense for the people whose information is implicated. Second, it creates a tech-neutral standard that will stay relevant as technology evolves.

5. **Participating Entity** - The term "participating entity" means an entity or person that collects, gathers, or uses consumer health information in any form or medium for non-personal purposes and that adopts this framework.

This has been drafted broadly in an effort to capture all entities that collect and/or use consumer health information. It no longer makes sense for consumers to have different rights depending on what entities hold their information.

6. **De-identified Data** - The term "de-identified data" means information that cannot reasonably be used to infer information about, or otherwise be linked to, an individual, a household, or a device used by an individual or household, provided that an entity in possession of consumer health information—
    a. Takes reasonable measures to ensure that the consumer health information cannot be reidentified, or associated with, an individual, a household, or a device used by an individual or household;
    b. Publicly commits in a conspicuous manner—
        i. To process and transfer the consumer health information in a de-identified form; and
        ii. Not to attempt to reidentify or associate the consumer health information with any individual, household, or device used by an individual or household; and
    c. Contractually obligates any person or entity that receives the information from the participating entity to comply with all of the provisions of this paragraph.

Similar to "Aggregated Data," it is critical to clearly define de-identified data within the framework. Properly de-identified data should pose fewer privacy risks to individuals and communities. To ensure that consumer privacy is protected, Section V below makes it clear that any participating entity seeking to utilize de-identified consumer health information must determine that the data is not individually identifiable by applying accepted methods and security practices. These reduced privacy risks allow de-identified data to be used in ways other identifiable data sets cannot under this framework.

7. **Publicly Available Information** - The term "publicly available information" means any information that -
    a. Has been lawfully made available to the general public from Federal, State, or local government records;
    b. Is published in a telephone book or online directory that is widely available to the general public on an unrestricted basis;

c. Is video, audio, or internet content published in compliance with the host site's terms of use and available to the general public on an unrestricted basis; or
d. A news media organization publishes to the general public on an unrestricted basis.

For the purposes of this definition, information is not restricted solely because there is a log-in requirement associated with accessing the information, or a fee of no more than $20 per month or per transaction. When a user of a social media service creates or shares information on that service, such information is restricted unless it is freely accessible by all users of the service.

Like many proposals, this framework recognizes that there is individual and societal value in the free flow of information and that even health data that has legitimately been made public may receive reduced protections. We have tried to craft this definition to capture truly public information while not being overly broad. We also clarify that traditional sources of news, like newspapers, whose digital presence may have a log-in and/or small cost associated with their service, is still considered well within the public sphere.

8. **Privacy Review Board** - The term "privacy review board" means an independent board that -
    a. Is comprised of at least three members;
    b. Has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and related interests;
    c. Includes at least two members who are not affiliated with the participating entity, not affiliated with any entity conducting or sponsoring the research, and not related to any person who is affiliated with any of such entities;
    d. Includes at least one member who is a consumer representative; and
    e. Does not have any member participating in a review of any project in which the member has a conflict of interest.

Review boards inject valuable, independent professional review for certain proposed uses of consumer health data. Large and consequential uses of consumer health information will benefit from this independent scrutiny. In an effort to stay consistent and not introduce a host of new terms or requirements, this definition is heavily influenced by similar provisions within HIPAA and its accompanying regulations.

9. **Research** - The term "research" means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

This definition is heavily influenced by similar provisions within HIPAA, the Common Rule regarding federal human subjects, and their respective regulations. This definition permits

public interest research to continue while avoiding a loophole that could be used to justify and type of commercial data research.

Collection and Processing of Consumer Health Information

I. Transparency and Notice

Transparency and notice serve two functions. First, both allow individual consumers to make informed decisions before they agree to have their health information collected, disclosed, or used. Second, transparency and notice requirements allow researchers, regulators, and advocates to track data use trends and better understand companies' practices. Because these purposes require a different level of detail, the framework requires two sets of notice. This approach provides consumers with the information they need without overwhelming them, while simultaneously providing more thorough information to be used in the public interest.

Elements of Notice:

A participating entity shall not collect, disclose, or use consumer health information unless it provides the following information to consumers before any data is collected, disclosed, or used—

1. Clearly identifies the types of health information that will be collected.
2. Clearly states the purpose(s) that any health information is collected for.
3. States if any health information will be disclosed, and if so, provides the user with the names of all the entities that will receive, license, or purchase the consumer health information.
4. States the reasons that any health information is disclosed.
5. Notifies consumers when policies and practices surrounding how their health information will be collected, disclosed, or used have changed.
6. Provides consumers with a description of the consumer's individual rights and a clear list of any consumer controls that a participating entity has made available.

Forms of Notice:

A participating entity that collects, discloses, or uses consumer health information shall, with respect to each service or product provided by the participating entity, publicly publish—

1. A consumer-facing policy that—
    a. Includes information regarding each element listed within the "elements of notice" section of this framework; and
    b. Must be written in a manner that is succinct and easily understandable to a consumer.

2. A complete second and more detailed policy that includes—
    a. The specific types of consumer health information collected;

b. The manner in which consumer health information is collected;
c. The purposes for the consumer health information collection;
d. The security and retention procedures for how the participating entity handles consumer health information; and
e. A detailed list of all third parties with whom the participating entity has disclosed or plans to disclose consumer health information.

Section 1 is designed to inform consumers as they engage with a participant's product. Section 2 is designed to provide more information for civil society groups, researchers, reporters, and regulators that wish to conduct oversight of the collection and use of consumer health information.

II. Consent

Elements of Consent:

Before a participating entity may collect or use consumer health information—

1. A participating entity must obtain affirmative express consent from a consumer that details the purpose and intended use from the individuals whose health information will be collected, disclosed, or used.
2. Affirmative express consent shall be freely given and nonconditioned.

A participating entity collecting, disclosing, or using consumer health information must limit the collection, disclosure, or use of consumer health information to only what the consumer has expressly consented to.

1. A participating entity must seek additional consent for any new collection, disclosure, or use of consumer health information outside the scope of any previous consumer consent.
2. A participating entity collecting, disclosing, or using consumer health information must provide consumers with the ability to revoke consent.
    a. A participating entity must stop the collection, disclosure, or use of health information once a consumer has revoked consent.

These provisions are drafted to require consumer consent around specific collections and uses of consumer health information as opposed to a simple blanket consent for a host of possible uses. It also includes important consumer rights to revoke consent later on.

III. Consumer Controls

Consumer Rights with Respect to Consumer Health Information:

1. Consumers' Right to Access, Correct, and Delete Consumer Health Information

a. A participating entity shall provide a consumer with a free, clear, and easy process for requesting personal consumer health information within the participating entity's possession.
b. A participating entity shall provide a consumer with a free, clear, and easy process for requesting corrections or deletions to any inaccurate information within the consumer health information within the participating entity's possession.
c. A participating entity shall make reasonable efforts to correct or delete a consumer's health information based upon a consumer's request for correction or deletion.
    i. When correction or deletion cannot occur, a participating entity shall provide the requesting consumer with an explanation as to why the correction or deletion request cannot be carried out.

2. Consumers' Portability Rights
    a. Where technically feasible, a participating entity shall make available a reasonable means for a consumer to transmit or transfer their health information that is retained by the participating entity to another participating entity in a structured, standardized, and machine-readable interoperable format, or otherwise download personal information for the consumer's own use.

3. The Use of Consumer Health Information to Train or be the Subject of Automated Systems or Processes
    a. A participating entity shall not collect, disclose, or use consumer health information to train or be the subject of any automated, algorithmic, or artificial intelligence application unless that entity has first:
        i. Obtained affirmative express consent from a consumer for the use of their health information in such applications, or
        ii. Subjected the consumer health information to be collected, disclosed, or used to a risk-based privacy assessment and any risks identified have been appropriately mitigated, and the use is consistent with a reasonable individual's expectations given the context in which the individual provided or authorized the collection, disclosure, or use of their consumer health information.
    b. Automated, algorithmic, or artificial intelligence applications, processes, and systems must be designed and implemented by the participating entity to mitigate potential algorithmic bias, including through design processes that regularly interrogate the variables and training data used, measures that ensure transparency and explainability, and routine auditing.

We have drafted this section to include several consumer rights that are consistent with existing domestic and international regulations and proposals.

IV. Obligations for Participating Entities

Currently, the burden of ensuring sufficient privacy protections around health data disproportionately falls on consumers. This portion of the framework focuses on data collection and use practices that ensure data is used for limited purposes consistent with consumer requests and expectations. We have also included data security provisions.

Relation to Existing Federal, State, and Municipal Laws and Regulations:

To the extent that any participating entity's collection, disclosure, or use of consumer health information is already governed by Federal, State, and Municipal laws or regulations, those legal obligations are not affected by this framework.

This section is intended to make clear that framework participants must follow all applicable laws and regulations in addition to offering consumers the higher level of protections included within the framework.

Permissible Collection and Use Practices for Consumer Health Information:

1. A participating entity—
    a. Shall not collect, disclose, or use consumer health information for any purpose other than what the data was originally collected, disclosed, or used for;
    b. Shall limit the amount of consumer health information collected, disclosed, or used to only what is necessary to provide the product or feature the consumer has requested,
    c. Shall take reasonable efforts to ensure the third parties and service providers with whom it shares consumer health information meet the obligations of this framework.

This section is intended to categorically prohibit secondary uses of health data that do not fall under one of the clearly defined exceptions to this framework. If a participating entity would like to offer a new product, functionality, or repurpose data for any reason, they must start the notice and affirmative consent process over. In no instance should terms of service serve as justification for secondary uses of data. Data collection and use limits carry through to third parties. Consumers should be protected without having to take additional steps to monitor how their data is being used by third parties.

This section is likely to curb some current behavioral advertising and commercial product development activities that do not avail themselves of one of the other exceptions like the use of de-identified data. We understand this approach is more stringent than other voluntary frameworks or legal standards, but believe health data warrants the protection.

Consumer Health Information Retention:

1. A participating entity -

a. Shall maintain consumer health information for a period of time only as long as necessary to carry out the purpose(s) for which the consumer health information was collected;
b. Shall delete all consumer health information once there is no longer a valid reason to retain it.

There should be clear and reasonable limits on the length of time consumer health information may be maintained by participating entities. Retention limits benefit both consumers and participants. Less data can lessen the impact of breaches and ensure that decisions are not made on stale, old, and incorrect data, and produces lower storage and security costs. These limits are consistent with limits in other existing proposals and regulations.

Prohibitions on the Use of Consumer Health Information to Harm or Discriminate Against Consumers:

1. A participating entity shall not collect, disclose, or use consumer health information when making eligibility determinations around housing, employment, healthcare, and other critical determinations.
2. A participating entity must ensure equal access and accommodation considerations when collecting, disclosing, or using consumer health information.

Consumer health information is inherently sensitive. It should not be collected, disclosed, or used in ways that harm, discriminate against, or limit consumer's access to critical life opportunities.

Security:

1. A participating entity shall establish and implement reasonable information security policies, practices, and procedures for the protection of consumer health information, taking into consideration—
    a. The nature, scope, and complexity of the activities engaged in by such participating entity;
    b. The sensitivity of any consumer health information at issue;
    c. The current state of the art in administrative, technical, and physical safeguards for protecting such information; and
    d. The cost of implementing such administrative, technical, and physical safeguards.
2. Requirements - The policies, practices, and procedures required in subpart (1) of this section must include the following:
    a. A written security policy with respect to the processing of such consumer health information.
    b. The identification of an officer or other individual as the point of contact with responsibility for the management of information security.
    c. A process for identifying and assessing reasonably foreseeable security vulnerabilities in any systems maintained by such participating entities that

contain such consumer health information, which shall include regular monitoring for vulnerabilities and breaches of security of such systems.

d. A process for taking action designed to mitigate against vulnerabilities identified in the process required by subparagraph (c)—which may include implementing any changes to security practices and the architecture, installation, or implementation of network or operating software—or for regularly testing or otherwise monitoring the effectiveness of the existing safeguards.
e. A process for determining if consumer health information is no longer needed and disposing of consumer health information by shredding, permanently erasing, or otherwise modifying the personal information contained in such data to make such consumer health information permanently unreadable or indecipherable.
f. A process for overseeing persons who have access to consumer health information, including through network-connected devices.
g. A process for employee training and supervision for implementation of the policies, practices, and procedures required by this subsection.
h. A written plan or protocol for internal and public response in the event of a breach of security.

This section imposes a "reasonable" security requirement on participants which is consistent with FTC enforcement and the laws in many states. Because "reasonable" is scaled to the sensitivity of the data, the way it is used, and the state of technology, participants' obligations will be commensurate with the business and engineering decisions they make. The processes required here are also flexible and outcome based which is usable for participants of all sizes and sophistication.

V. Exceptions

Nothing in this framework shall limit participating entities from:

1. Engaging in practices that utilize consumer health information when necessary and solely for archiving purposes in the public interest, scientific or historical research purposes, or statistical purposes that adhere to commonly accepted ethical standards and laws,
    a. With affirmative express consent from a consumer; or
    b. For research that has been reviewed and approved by a privacy review board; or
    c. For research utilizing de-identified consumer health information, provided that—
        i. A participating entity may utilize de-identified consumer health information for research in the public interest without consumer consent only after it determines that consumer health information is not individually identifiable. This determination shall be made by a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable, who:

1. Applying such principles and methods, determines that the risk is very small that the consumer health information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and
2. Documents the methods and results of the analysis that justify such determination.

d. For research utilizing aggregated consumer health information, provided that—
   i. A participating entity may utilize aggregated consumer health information for research in the public interest without consumer consent only after it—
      1. Determines that the consumer health information to be used only relates to a group or category of individuals or devices that does not identify and is not linked or reasonably linkable to any individual, and
      2. Documents the methods and results of the analysis that justify such determination.

2. Engaging in commercial, academic, or research practices that utilize publicly available consumer health information so long as—
   a. A participating entity does not collect, disclose, or use publicly available consumer health information when making eligibility determinations around housing, employment, and other critical determinations; and
   b. A participating entity ensures equal access and accommodation considerations when collecting, disclosing, or using publicly available consumer health information.
3. Using or disclosing consumer health information to a medical professional or health care provider without consumer consent if that participating entity, in good faith—
   a. Believes that an emergency involving danger of death or serious physical injury to any person requires use or disclosure relating to the emergency, and
   b. Believes that any recipient of this information is in a position to address, rectify, or prevent the emergency.
4. Engaging in practices that utilize consumer health information when necessary and solely for purposes of—
   a. Detecting and preventing security incidents, identity theft, or fraud or protecting against malicious or deceptive activity;
   b. Identifying or repairing errors that impair existing intended functionality;
   c. Complying with a Federal, State, or local law, rule, or other applicable legal requirement, including disclosures pursuant to a court order, subpoena, summons, or other properly executed compulsory process.
   d. Addressing health misinformation or moderating content or accounts to prevent harm to consumers.

The framework should include very limited exceptions that permit the collection, use, and sharing of health data without consent or for secondary purposes. Mindful of how exceptions

can undercut the effectiveness of a framework, these provisions borrow from long-standing laws that attempt to balance the equities between individual privacy, societal benefits from the use of this data, and participant needs to process data to deliver the service or product requested by an individual.

Proposed Framework Structure: Self-Regulatory Program

For any follow up questions, kindly contact Alice Leiter at eHI (alice@ehi.org)

The proposed program is one of accountability: a self-certification program designed to hold member companies to a set of standards separately developed through a multi-stakeholder process. The program would accept individual companies as members.[2] These members would undergo a thorough onboarding review at enrollment, be educated as to the self-regulatory framework, publicly commit to complying with it, and submit to annual assessments. Additionally, active "spot-check" monitoring would be done on a random sample of members throughout each year. Companies would hold themselves out to the public as a "XXX Health Data Participant" (name TBD).

User fees would be collected to maintain this program, and the amount of the fee would be on a sliding scale – likely based on the size of the company in terms of gross sales.

Relevant components/details of this program would include:

- Robust standards governing the program's onboarding reviews, annual compliance assessments, and ongoing monitoring of participant companies;
- Criteria to ensure that the reviews and assessment conducted by the program are independent of program's administrative and financial functions;
- A public commitment by each company to follow the program's standards;
- Maintenance by the program of a dedicated, public-facing website describing the program's goals and requirements, listing participating covered organizations, and providing an effective method for consumers to ask questions and file complaints about any program and/or any participating covered organization;
- A standardized set of privacy rules, that include:
    - A broad, use-based, definition of consumer health information;
    - Clear notice requirements;
    - Greater consumer access and control of their health information; and
    - Articulated appropriate uses and obligations surrounding the collection and use of consumer health information.
- An annual report by the program to the public detailing the program's activities and effectiveness during the preceding year in obtaining compliance by participating covered organizations and in taking meaningful disciplinary action for non-compliance.

[2] Included entities will be any company that collects, uses, or processes health-related personal data. These would include: hardware manufacturers; App developers; website publishers third-party data management, brokering, collection, or use outfits; potentially businesses/employers that rely on third-party health technology in order to maintain health of their workers.

Enforcement could include:

- Independent monitoring by program staff or other authorized evaluators, including publicly announced cases;
- Active complaint-gathering process;
- Requirement to develop a corrective action plan (CAP);
- Process to lose certification if CAP fails
- Penalties for persistent or willful non-compliance with the law and the program's standards, such as suspension or dismissal from the program, and/or referral to the FTC and/or state AG;
- Potential for FTC and/or state AG enforcement of violation of agreed to industry agreement; and
- A dispute resolution mechanism for resolving consumer complaints or complaints by another company based on the program's standards about non-HIPAA health data and potentially providing consumers with redress for violations.

This type of self-certification program would help to level the playing field among businesses, fostering a unified set of privacy practices that are responsive to recent regulation (the standards would presumably ensure compliance with the most stringent and/or far-reaching state laws), while raising the bar for consumer privacy in an area of great personal sensitivity. The critical difference between this program and a more passive pledge-style or "best practices" program is the inclusion of rigorous onboarding and ongoing accountability assessments, all of which are designed to elicit full compliance from well-intentioned actors and prevent bad actors from falsely shielding their inappropriate conduct behind a pledge Significantly, such a program could be easily converted into a safe harbor-style accountability mechanism in future legislation, giving it lasting utility even should new laws come about.

We aim to incorporate as much consumer input as possible in the establishment and operationalization of this program, with emphasis on its functioning as a bridge to legislation, rather than a final solution to the issue of under-protected data. In order for this program to be successful, it will need widespread consumer buy-in and trust, and the best way to achieve this is to involve consumers and consumer advocates in the design of the program itself.

Finally, although this program would depend on participation fees for its ongoing operations, it would require seed capital to establish initial operations. Given this, combined with a significant number of outstanding logistical issues, we see significant value in housing this program in an existing organization with established infrastructure and experience running self-regulatory programs, such as BBB National Programs.

How to Submit Feedback

We are looking for feedback on all aspects of the *Draft Framework*. Comments will be accepted until **Friday, September 25, 2020.**

To submit comments, please mail Alice Leiter at eHI (alice@ehidc.org) or Andy Crawford at CDT (acrawford@cdt.org), or visit https://www.ehidc.org/resources/draft-consumer-privacy-framework-health-data.