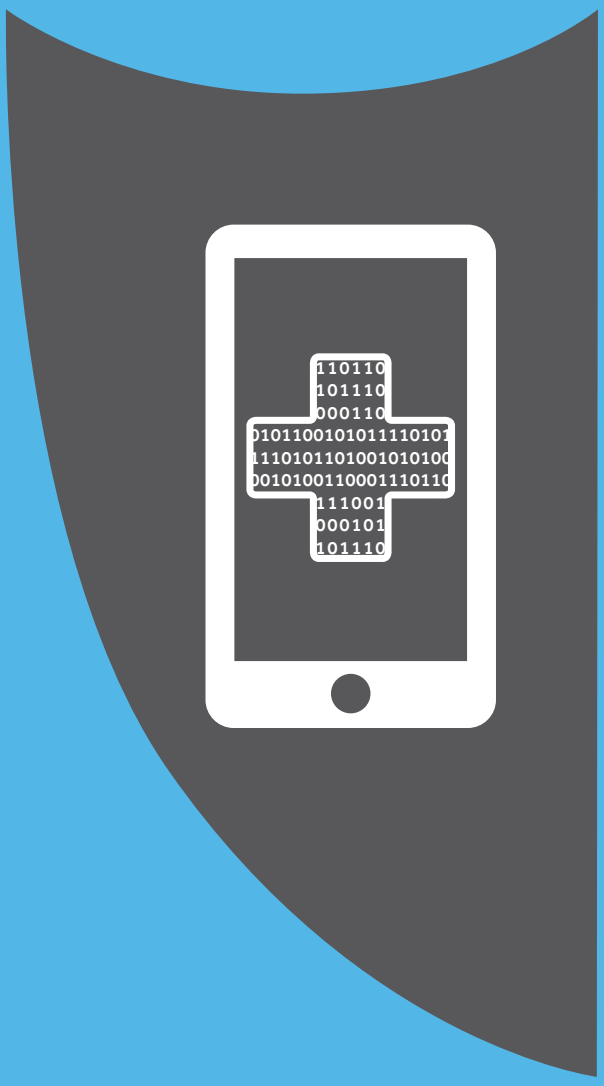

Proposed Consumer Privacy FRAME-WORK for Health Data

FEBRUARY 2021

CENTER FOR DEMOCRACY & TECHNOLOGY

EXECUTIVES FOR HEALTH INNOVATION

About Center for Democracy & Technology

The Center for Democracy & Technology is a 25-year-old nonprofit, non-partisan organization working to promote democratic values by shaping technology policy and architecture. For more information, visit cdt.org.

About Executives for Health Innovation

Executives for Health Innovation (EHI) , formerly eHealth Initiative (eHI), convenes executives from every stakeholder group in healthcare to discuss, identify, and share best practices to transform the delivery of healthcare using technology and innovation. EHI, along with its coalition of members, focuses on education, research, and advocacy to promote the use and sharing of data to improve healthcare. Our vision is to harmonize new technology and care models in a way that improves population health and consumer experiences. EHI has become a go-to resource for the industry through its Executive Resource Center. For more information, visit ehidc.org.

Acknowledgements

This framework is made possible with the support of the Robert Wood Johnson Foundation, and with assistance from our Steering Committee.

Special thanks to members of our two work groups for their invaluable engagement help and for their guidance. A list of select Steering Committee members can be found in the Appendix.

Proposed Consumer Privacy Framework for Health Data

Table of Contents

Executive Summary

Introduction and 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 such as doctors and insurance companies. However, with the rise of wearable devices, health and wellness apps, online services, and the Internet of Things, extraordinary amounts of information reflecting mental and physical well-being are created and held by entities that are not bound by HIPAA obligations. This issue has only gained importance, as new regulations finalized in the spring of 2020 will also ease and promote the movement of previously HIPAA-covered medical records into this commercially facing, non-HIPAA-covered and unregulated space.[1] The novel coronavirus has also thrust the issue of patient data privacy to the forefront, as efforts to trace and combat the spread of the virus have brought with them the relaxation of some federal privacy protections as well as increased data collection and use.

Project Goals and Process

With funding from the Robert Wood Johnson Foundation, Executives for Health Innovation (EHI), and the Center for Democracy & Technology (CDT) collaborated on a Consumer Privacy Framework for Health Data, with invaluable engagement and help from a steering committee of leaders from healthcare entities, technology companies, academia, and organizations advocating for privacy, consumer, and civil rights.

This steering committee helped guide eHI and CDT during the development of this framework. Specifically, the framework consists of a set of detailed use, access, and disclosure principles and controls for health data that are designed to address the gaps in legal protections for health data outside HIPAA's coverage. The framework also includes a proposed self-regulatory program to hold companies accountable to such standards. Non-HIPAA-covered entities would voluntarily hold themselves to a set of standards and subject themselves to potential enforcement mechanisms beyond current Federal Trade Commission (FTC) processes. Even outside this program, the authors hope that the substantive standards will serve as a benchmark to shape industry conduct and influence companies' approaches to ensure users' health data is protected.

[1] 85 Fed. Reg. 25642 (May 1, 2020) and 85 Fed. Reg. 25510 (May 1, 2020). For a comprehensive review of the current legal landscape governing health data and the gaps in protection for the same, please see Belfort, R., Dworkowitz, A., Bernstein, William S., Pawlak, B. and Yi, P. *A Shared Responsibility: Protecting Health Data Privacy in an Increasingly Connected World*, June 2020, available at http://www.manatt.com/Manatt/media/Media/PDF/White%20Papers/Healthcare-Whitepaper-RWJF-Protecting-Consumer-Health-Data-Privacy-in-an-Increasingly-Connected-World_e.pdf (Manatt White Paper).

The standards emphasize transparency, accountability, and appropriate limitations on health data collection, disclosure, and use. Importantly, the standards:

1. Move beyond outdated models that place too much emphasis on notice and consent and fail to articulate data use limits;
2. Cover all information that can be used to make inferences or judgments about a person's physical or mental health; and
3. Cover all non-HIPAA-covered entities that collect, disclose, or use consumer health information, regardless of the size or business model of the covered entity.

With respect to the self-regulatory program, the framework seeks to balance the need for enforcement mechanisms that will effectively hold companies responsible and promote consumer trust, while ensuring the program is workable enough for potential participating entities to join. This is a challenging balance, which the authors know will rely on entities participating in good faith.

Importantly, this proposal is **not** designed to be a replacement for new and necessary comprehensive data privacy legislation. Indeed, we believe strongly in the need for such a law and support all efforts to date that have served to build momentum for one. Given that congressional action is likely some time away and would take additional time to go into effect, this effort is designed to build support for best practices and enable us to take what action we can now, in the interim, to shore up protections for non-HIPAA-covered health data. We hope that some of the tenets of our proposal can and will be helpful to federal lawmakers in their future efforts.

Value of This Proposal for Different Stakeholders

Consumers. This model raises the bar for consumer privacy. Some existing best practices and voluntary frameworks define health information quite narrowly and do not cover all 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 transparency and consent remain important elements within the framework, many of the core privacy-protecting provisions of this framework are focused on how consumer health information is collected, disclosed, and used. Although older 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 every day given the proliferation in the number of available technologies and the length, details, and lack of clarity of their terms of service. By putting clear restrictions on the collection, disclosure, and use of data, the proposed framework shifts the burden of privacy risk off users and onto the companies.

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

Non-HIPAA-covered technology companies 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 legal risks in a world where consumers and enforcement agencies expect more from companies that handle data. Participating entities may also see significant reputational and thus commercial benefit in an increasingly crowded market.

Finally, this model has the potential to provide some compliance certainty for participants. By adopting more forward-looking privacy practices, companies and organizations will avoid the gray or evolving areas of existing laws. Especially for smaller or newer companies having difficulty fully understanding their numerous federal and state legal obligations, which can often be unclear and/or conflicting, compliance with our framework's standards would provide some assurance that participants are staying ahead of various potential federal and state requirements.

Regulators and oversight bodies. Congress, the FTC and their state-level counterparts will benefit from companies committing to a common set of publicly available data practices. This commitment will allow these governmental bodies to enforce these practices, which will be more explicit than many existing company privacy policies. Instead of engaging in complicated investigations and balancing tests, these entities will be able to measure compliance more easily and better allocate their limited enforcement resources.

Traditional healthcare system entities. Finally, although this framework is geared toward companies that operate outside the traditional healthcare system and thus are not subject to the obligations and protections of HIPAA, our framework will benefit HIPAA-covered entities as well. The framework recognizes the importance of research and establishes clear standards for when research relying on consumer health information is permitted.

Moreover, the release of the Centers for Medicare & Medicaid Services and Office of the National Coordinator for Health Information Technology final rules regarding interoperability and information-blocking means that consumers will soon have greater access than ever to their own health data. By virtue of the framework, providers and consumers alike will have a far easier time choosing applications for this data transfer that adhere to meaningful and robust privacy practices.

Substantive Standards and Policy Rationale

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

In addition to the text of the framework, throughout this section we include blue fields containing summaries of the feedback we received, policy rationale, and explanations for each section.

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 that:
            (A) Is written concisely and in an easy-to-understand manner that is accessible to all consumers; and
            (B) Includes clear headings 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.

Much of the data covered by this framework is inherently sensitive on its own or when used in certain ways. When the collection, use, or sharing of certain data is conditioned on consent, it is crucial that consent be meaningful. It has been repeatedly documented that terms that appear in lengthy privacy policies do 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 (for example, with a condition that unnecessary data be collected as part of a sale). 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 that would cover consumer health information.

2. **Aggregated Health Data** - The term "aggregated health data" means health data that relates to a group or category of individuals 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 a household.

   A participating entity in possession of aggregated health data shall:

   a. Take reasonable measures to safeguard the aggregated health data from reidentification, including the adoption of technical and organizational measures to ensure that the information is not linked to any individual, household, or device used by an individual or a household;

   b. Publicly commit in a conspicuous manner not to attempt to reidentify or associate the aggregated health data with any individual, household, or device used by an individual or a household; and

   c. Contractually require the same commitments from recipients of all transfers of aggregated health data.

This framework recognizes that properly aggregated data may pose fewer privacy risks to individuals, families, and communities. As a result of that reduced privacy risk and the offsetting public benefit of some uses of aggregated data, this framework permits certain uses of aggregated data for research purposes or internal analysis (see Section V). Importantly, aggregation is not a silver bullet in protecting individual privacy. This framework requires covered entities to safeguard aggregated health data from reidentification and to contractually require the same commitment from any entity that receives the aggregated data.

We received comments asking for greater clarification around the definitions of both aggregated and de-identified data. It is critical for these definitions to be clear because aggregated and de-identified data sets are subject to different use limitations under the framework. To address these comments, the definitions of aggregated and de-identified health information have been modified to make clear that they are not subsets of consumer health information. Additional clerical edits have also been made to these definitions to ensure consistency of terms and approach.

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

Comments received about this section asked whether minors are included within the definition of consumer. Minors face the same potential harms when their health data is misused or used in unintended ways and should have the same protections as everyone else under the framework. To address this feedback, we have now included a reference to minors within the definition to clearly indicate that they are included.

4. **Consumer Health Information** - The term "consumer health information" means:
    a. Any information, recorded in any form or medium, that is created or received by an entity and:
        i. Relates to or is used to determine, predict, or estimate the past, present, or future physical or mental health condition of an individual; or
        ii. Relates to the provision of healthcare to an individual.
    b. The following data sets regardless of the purpose or outcome of the collection, disclosure, or use:
        i. Genetic data;
        ii. Data that reflects a particular disease or condition;
        iii. Data that reflects any substance use disorder;
        iv. Data that reflects reproductive health; and
        v. Data that reflects disability.[2]
    c. Exclusions - Consumer health information does not include:
        i. Protected health information (PHI) held or maintained by a HIPAA-covered entity or business associates acting for the covered entity.

[2] As defined under the Americans with Disabilities Act of 1990, available at https://www.ada.gov/pubs/adastatute08.htm.

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. Examples of some of these data sets are as follows:

- Data that reflects racial and ethnic origin;
- Biometric data; and
- Data that reflects sexual orientation.

Subsection (b) declares that certain sensitive health information shall always be subject to the framework, regardless of the context of its use.

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.

We received a number of thoughtful and detailed comments about this section. Several of the comments focused on the broad nature of the definition. We took this feedback seriously. To address these points, the definition has been refined to clarify when certain data sets, such as racial and biometric data, will be treated as consumer health information. These edits focus the framework's protections on data sets that are collected, disclosed, and used for health purposes while still recognizing that certain types of data are always consumer health information. Finally, the addition of the exclusion section is intended to make clear that this framework is focused on consumer health information that is not covered by HIPAA.

5. **De-identified Health Data** - The term "de-identified health data" means health data 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 a household.

   A participating entity in possession of de-identified health data shall:

   a. Take reasonable measures to safeguard the de-identified health data from reidentification, including the adoption of technical and organizational measures to ensure that the information is not linked to any individual, household, or device used by an individual or a household;

   b. Publicly commit in a conspicuous manner not to attempt to reidentify or associate the de-identified health data with any individual, household, or device used by an individual or a household; and

   c. Contractually require the same commitments from recipients of all transfers of the de-identified health data.

Properly de-identified data may pose fewer privacy risks to individuals, families and communities. As a result of that reduced privacy risk and the offsetting public benefit of some uses of de-identified health data, this framework permits certain uses of this data for research purposes or internal analysis (see Section V). De-identification is not a silver bullet in protecting individual privacy. This framework requires covered entities to safeguard de-identified health data from reidentification and to contractually require the same commitment from any entity that receives the de-identified data.

We received a number of comments about this definition that are discussed under the definition of aggregated health data above. Additionally, we received comments specifically about de-identified data. Those comments focused on de-identified health data carrying a greater potential to be reidentified compared to aggregated health data. While it is not possible to completely eliminate the risk of reidentification, the definition requires participating entities to not reidentify this data.

6. **Participating Entity** - The term "participating entity" means an entity that collects, gathers, or uses consumer health information in any form or medium for nonpersonal 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.

We received some comments seeking greater clarification regarding how this framework would apply to entities that may have certain data sets that are covered by HIPAA while others are not. This framework is focused on non-HIPAA-covered data and is intended to increase privacy protections around data sets that currently fall outside HIPAA's coverage while not creating overlapping or conflicting requirements for participating entities.

7. **Privacy Review Board** - The term "privacy review board" means an independent board that:
    a. Is composed 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 with experience working in the consumer health context; and
    e. Does not have any member participating in a review of any project in which the member has a conflict of interest.

    For the purposes of this definition, an institutional review board (IRB) or a privacy board as contemplated under the HIPAA Privacy Rule shall satisfy this definition so long as the IRB or privacy board meets the composition requirements of this provision.

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.

We received comments regarding the composition of privacy review boards. Because the framework is focused on health information, any consumer representative must have experience working on consumer health issues to best protect consumers' rights. The definition also makes it clear that IRBs and privacy boards satisfy this requirement so long as they meet each element within the definition.

8. **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 an 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. Is published by a news media organization to the general public on an unrestricted basis.

    For the purposes of this definition, information is not restricted solely because there is a login requirement associated with accessing the information or a fee. When a user of a social media service creates or shares information on that service, such information is restricted unless it is freely accessible to anyone using 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 may receive reduced protections when it has legitimately been made public. 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, such as newspapers, whose digital presence may have a login and/or small cost associated with their service, are still considered well within the public sphere.

We received several comments regarding publicly available information. Specifically, to address comments about information that requires a fee for access, we eliminated a specific dollar amount in an effort to account for several services that have varying fee schedules.

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 any type of commercial data research.

Collection and Processing of Consumer Health Information

I. 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.

A. 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 and 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.

B. Privacy and Security Protections

A participating entity shall offer the same levels of privacy and security protections and data rights and controls to all consumers, regardless of whether the consumer is paying for services or receiving them for free.

C. Permissible Collection and Use Practices for Consumer Health Information

A participating entity:

1. Shall not collect, disclose, or use consumer health information for any purpose other than the purpose for which the data was originally collected, disclosed, or used;
2. 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; and
3. Shall take reasonable efforts to contractually obligate third parties and service providers with whom it discloses consumer health information to also 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 or functionality or repurpose data for any reason, it must seek affirmative consent for that new use. 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, such as the use of de-identified data. We understand this approach is more stringent than other voluntary frameworks and legal standards, but we believe health data warrants the protection.

To address comments regarding the obligations section, we have clarified that a covered entity shall take reasonable efforts to contractually obligate third parties and service providers. This approach better aligns the framework with similar privacy protections found in other proposals and industries, and provides participating entities and consumers with greater assurance that the framework's protections carry though to third parties.

D. Consumer Health Information Retention

A participating entity:

1. 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; and
2. 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.

E. 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 to discriminate against consumers.
2. A participating entity shall not collect, disclose, or use consumer health information when making significant eligibility determinations, including housing, employment, healthcare, and other significant determinations.
3. A participating entity shall not draw inferences from a consumer's refusal to use or cessation of use of a platform, product, app, or digital health tool that could lead to discrimination, stigmatization, harmful profiling, or exploitation.

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

To address comments regarding the use of consumer health information to harm consumers, we have included an additional provision within this section. Specifically, the additional section makes it clear that a consumer's decision to not use or to stop using a specific product or service shall not have any negative or harmful consequences.

F. 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 collection, retention, and use 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 whether consumer health information is no longer needed and for 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; and

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 that 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.

II. Consumer Controls

A. Consumer Rights With Respect to Consumer Health Information

1. Consumers' Rights 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 and receiving a list of all other affiliates, service providers, and third parties that have received, licensed, or purchased their consumer health information:

        i. If a participating entity has shared, licensed, or sold consumer health information to another entity that contracts with one or more individuals who act as independent contractors to provide a benefit (such as transportation, deliveries, or another immediate benefit) directly to a consumer, the participating entity must identify the other entity, but need not list or identify any end-service providers.

    c. 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 in the participating entity's control.

    d. A participating entity shall make reasonable efforts to correct or delete a consumer's health information based on a consumer's request for correction or deletion.

    e. 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.

To address comments regarding consumers' ability to receive information about all other entities that have received, licensed, or purchased their consumer health information, this section now provides consumers with a clear mechanism to obtain this information. The additions to this section are also necessary because of modifications made to the transparency requirements above that now require that consumers receive information about the types of entities that will receive, license, or purchase their consumer health information. This addition strikes a balance between consumers' interests and the compliance obligations of participating entities.

Additionally, we received comments that raised concerns regarding how information that was at one time HIPAA-covered data (PHI) should be treated under this section. Specifically, commenters raised concerns that a consumer's medical records, records that were once covered by HIPAA and may well be shared in the future with HIPAA-covered entities, should only be annotated and not subject to broader correction and/or deletion requirements. While we recognize these concerns, this framework is designed to operate outside HIPAA and give consumers greater control over their health information. We encourage participating entities that collect, disclose, or use these types of records to ensure that these consumer rights are made clear to everyone via the framework's transparency requirements. Moreover, medical professionals who may receive this type of consumer health information should appreciate that the consumer, and not a HIPAA-covered entity, is deciding what information they are sharing and proceed accordingly.

2. Consumers' Portability Rights

    a. Where technically feasible, a participating entity shall make available a reasonable means for a consumer to download their health information that is retained by the participating entity in a structured, standardized, and machine-readable interoperable format 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 (AI) 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, 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. If the consumer health information served as an input for an automated system or process, any resulting data that is produced or results from that automated system or process shall be considered consumer health information if:

i. The resulting data relates to or is used to determine, predict, or estimate the past, present, or future physical or mental health condition of an individual;

ii. The resulting data relates to the provision of healthcare to an individual; or

iii. The resulting data includes:

(A) Genetic data;

(B) Data that reflects a particular disease or condition;

(C) Data that reflects any substance use disorder;

(D) Data that reflects reproductive health; or

(E) Data that reflects disability.

c. Automated, algorithmic, or AI 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.

To address comments regarding the use of data sets produced by automated, algorithmic, or AI applications, processes, and systems that used consumer health information in the creation of those subsequent data sets, this section has been modified to align with the framework's definitions to clarify when those new data sets shall be treated as consumer health information.

III. Notice and Transparency

Section I establishes data collection and use practices that ensure consumer health data is used for limited purposes consistent with consumer requests and expectations. This section builds on those critical protections and is designed to empower consumers with the information they need.

Notice and transparency serve two complementary functions. First, timely and meaningful notice allows individuals to make informed decisions before they agree to have their health information collected, disclosed, or used. Second, ongoing transparency requirements allow individuals to revisit a participating entity's data policies at a time of their convenience or keep up to date with changing data uses. It also allows researchers, regulators, and advocates to track data use trends and better understand companies' practices. Because these purposes require different levels of detail, the framework requires participating entities to prepare two sets of information. This approach provides consumers with the information they need without overwhelming them, while simultaneously providing more thorough information to be used over time or in the public interest.

A. Notice

A participating entity shall not collect, disclose, or use consumer health information as permitted under Section I unless it first:

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. Clearly states the data retention policies that will apply to the consumer's health information;
4. States whether any health information will be disclosed and, if so, provides the user clear information about the specific types of entities that will receive, license, or purchase the consumer health information;
5. States the reason(s) any health information is disclosed;
6. Commits to promptly notifying consumers when policies and practices surrounding how their health information will be collected, disclosed, or used have changed; and
7. Provides consumers with a description of their individual rights and a clear list of any consumer controls that a participating entity has made available.

To address comments regarding greater transparency around data retention, this section now contains a provision requiring participating entities to tell consumers how long they will retain the consumers' health information. Retention information can help consumers make informed choices when selecting services and also allow consumers to act should they wish to obtain a copy of their health information before it is no longer retained by an entity.

We also received several comments regarding the framework's notice provisions. Specifically, commenters noted that it may not be possible and/or may be overly burdensome to identify every entity that may receive a consumer's health information at the time they consent to using a product. To address this, the notice provision now requires participating entities to provide information about the types of entities that receive consumers' health information. This modification still permits consumers to make informed decisions when engaging a product for the first time. If a user wishes to know the names of all the entities that may collect, use, or share their information, they may find them in the transparency report required by the next section.

B. Transparency

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

1. A consumer-facing policy that:
    a. Includes information regarding each element listed within the "Notice" section of this framework; and
    b. Is written in a manner that is succinct and easily understandable to a consumer.
2. A complete second and more detailed policy that includes:
    a. Each element listed within the "Notice" section of this framework;
    b. The manner in which consumer health information is collected; and
    c. A detailed list of all affiliates, service providers, and third parties with whom the participating entity has disclosed or plans to disclose consumer health information.

With regard to obligations of a participating entity to list other entities that will receive, license, or purchase consumer health information, if the other entity is one that contracts with one or more individuals who act as independent contractors to provide a benefit (such as transportation, delivery, or another immediate benefit) directly to a consumer, the participating entity must identify the other entity, but need not list or identify any end-service providers.

As a result of the comments we received, this section now includes additional clarity around situations where covered entities work with partners that use independent contractors to provide a benefit. For example, a participating entity need not list the names of individual independent contractor(s) (such as a delivery person); it need only provide the name of the service provider partner.

IV. Consent

Participating entities must obtain a consumer's affirmative express consent prior to any collection, disclosure, or use of consumer health information permitted under Section I. Consent adds an important layer of protection and consumer control within the framework by permitting the individual consumer to decide whether or how their health information will be collected, disclosed, or used.

These provisions are drafted to require consumer consent for 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.

It is important to note that nothing in this section allows "consent" to override any of the categorical prohibitions and obligations in Section I. For example, a person cannot consent to being discriminated against, to having their data used or shared for prohibited secondary purposes, or to being subjected to a pay-for-privacy scheme.

A. Elements of Consent

In addition to the obligations for participating entities in Section I, before a participating entity may collect, disclose, or use consumer health information:

1. A participating entity must obtain affirmative express consent from a consumer;
2. 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;
3. A participating entity may seek to obtain affirmative express consent from a consumer for continued, ongoing, or periodic collection, disclosure or use of consumer health information when both the purpose and intended use of consumer health information is the same for every instance of collection, disclosure, or use; and
4. Affirmative express consent shall be freely given and nonconditioned.

B. Revocation of Consent

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

We received numerous comments regarding the framework's consent provision, and recognize that questions around consent and its continued applicability and utility are difficult. While this framework is designed to move beyond existing consent-centric regimes by placing real limits around the collection, disclosure, and use of consumer health information, there are instances where consumers' control of their data matters. Given the sensitivity of the covered health information protected by this framework, consumers must consent before their health data is collected, disclosed, or used.

Additionally, we received comments and questions regarding the frequency of consent required under this section. To address this, we added additional clarifications that make it clear that a single consent is sufficient for continued, ongoing, or periodic collection, disclosure, or use of consumer health information, so long as the purpose and intended use of consumer health information is the same for every instance. Consumers and participating entities should not be overburdened with redundant consent requests.

V. Exceptions

Nothing in this framework shall limit participating entities from:

1. Engaging in practices that use consumer health information when necessary 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;
    b. Provided that the research has been reviewed and received written approval by a privacy review board; or
    c. If the research uses aggregated health data, provided that:
        i. A participating entity may use aggregated health data for research without consumer consent only after it:

(A) Determines that the aggregated health data to be used only relates to a group or category of individuals or devices and does not identify and is not linked or reasonably linkable to any individual;

(B) Documents the methods and results of the analysis that justify such determination; and

(C) Produces a publicly available statement explaining the participating entity's practices regarding the general methods used for aggregating consumer health information;

d. If the research uses de-identified health data, provided that:

i. A participating entity may use de-identified health data for research without consumer consent only after it determines that the data 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:

(A) Applying such principles and methods, determines that the risk is very small that the de-identified health data 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;

(B) Documents the methods and results of the analysis that justify such determination; and

(C) Produces a publicly available statement explaining the participating entity's practices regarding the general methods used for rendering consumer health information not individually identifiable.

2. Engaging in commercial, academic, or research practices that use only publicly available consumer health information.

3. Using or disclosing consumer health information to a medical professional or healthcare provider without 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 the recipient of this information is in a position to address, rectify, or prevent the emergency; and

c. If a participating entity uses this emergency exception, it shall promptly notify the consumer whose health information was disclosed.

4. Engaging in practices that use consumer health information when necessary and solely for the purposes of:
    a. Detecting and preventing security incidents, identity theft or fraud, or protecting against malicious or deceptive activity;
    b. Performing system maintenance, diagnostics, debugging, or error repairs to ensure or update the functionality of a product or service;
    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; or
    d. Addressing health misinformation or moderating content or accounts to prevent harm to consumers.
5. Collecting, disclosing, or using data:
    a. About an individual in the course of the individual's employment or application for employment (including on a contract or temporary basis), provided that such data is retained or used by the participating entity or the participating entity's service provider solely for purposes necessary for the individual's employment or application for employment;
    b. That is emergency contact information for an individual who is an employee, contractor, or job applicant of the participating entity, provided that such data is retained or used by the participating entity or the participating entity's service provider solely for the purpose of having an emergency contact for such individual on file; or
    c. About an individual (or a relative of an individual) who is an employee or former employee of the participating entity for the purpose of administering benefits to which such individual or relative is entitled on the basis of the individual's employment with the participating entity, provided that such data is retained or used by the participating entity or the participating entity's service provider solely for the purpose of administering such benefits.
6. Engaging in limited commercial product development:
    a. With affirmative express consent from a consumer for this specific use, provided that it:
        i. Uses aggregated health data or de-identified health data;
        ii. Complies with the provisions of the "Prohibitions on the Use of Consumer Health Information to Harm or Discriminate Against Consumers" section of this framework;

iii. Meets the requirements of the "Notice" and "Transparency" sections of this framework for this specific and limited use; and

iv. Does not share any consumer health information, de-identified health data, or aggregated health data used in that development with a third party.

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 participants' needs to process data to deliver the service or product requested by an individual.

To address comments regarding the use exceptions for aggregated and de-identified data, modifications were also made to this section to keep terms consistent throughout the framework. Additionally, to address comments regarding employee data, subsection 5 was added to clearly list limited exceptions for the use of employee data. These points reiterate the provisions of the newly added employee data definition so that employers are not overly burdened when using data about their employees for purely administrative functions.

We received several comments regarding how participating entities should handle employee data under the framework. In response, we have included a new exception that is designed to identify limited, specific instances where data may be collected, disclosed, or used outside the framework's general provisions for the limited employment-related purposes enumerated here. Data about employees that is collected, disclosed, or used for any other purpose falls outside this exception and is subject to the same protections as the covered data of any other person.

Finally, we received several comments surrounding the use of consumer health information for commercial product development. We recognize that consumer health information can help entities develop innovative new products and services. However, these commercial benefits must be properly balanced with consumers' rights.

In an effort to strike a balance and permit limited commercial use, we have added language designed to promote strong consumer privacy protections when consumer health information will be used by a participating entity solely for commercial purposes. Specifically, to best protect consumer privacy, this section limits commercial development to aggregated and de-identified data. It incorporates the framework's antidiscrimination and transparency provisions to ensure consumers will not be harmed and will know how their data will be used. Since this is a new exception, we look forward to continuing to work with our partners and the public on this important provision.

Proposed Self-Regulatory Program: Policy Rationale

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

Numerous efforts in recent years have successfully developed comprehensive codes of conduct and terms of service to protect consumer privacy.[3] Rather than duplicate such efforts, we decided to pursue a more formal, tangible, and meaningful accountability structure: a self-regulatory program for non-HIPAA-covered entities that collect, use, and share health data. This proposal would establish a voluntary self-certification program led by an independent, third-party organization. This reduces the potential for bias and lax internal policing, increases the possibility for meaningful adherence to privacy practices, and ensures consequences for nonadherence.

Addressing Consumer Trust

While we grappled with options to protect consumer privacy, a self-regulatory model arose as the most effective option available in the current environment. Perhaps most relevant to this project, self-regulation can engender trust: "...[T]he most important goal of any self-regulatory system is building consumers' trust in its participants. Self-regulation often arises in response to erosion of trust.... Laws rarely achieve the goal of building trust, because they merely set a baseline for compliance."[4] Further, self-regulatory programs can be nimbler and more flexible than government regulation.[5]

Successful self-regulatory programs can create trusted environments by "setting standards that only responsible organizations can meet. Participants in the self-regulatory system obtain the benefit of differentiating themselves from others whose conduct, while it may be legal, is not exemplary."[6] Moreover, public reporting of compliance with the standards provides a level of transparency and accountability that further engenders trust.

Self-regulation incentivizes competitors to monitor each other for compliance with the agreed-to standards. It provides consumers with a clear and straightforward way to file complaints. Most important, self-regulatory programs are based on a neutral enforcement mechanism.

[3] *See* Manatt White Paper at pp. 16–17. This paper provides an in-depth discussion on self-regulation, what models have been implemented and how they have worked in other industries, and how one might work in healthcare. We have pulled out key points for this policy rationale but encourage a full read of the paper for a more thorough look at the benefits and particulars of a self-regulatory model for non-HIPAA-covered entities.

[4] Boulding, M. "Self-Regulation: Who Needs It?," *Health Affairs*, Volume 19, Number 6 (2000), available at https://www.healthaffairs.org/doi/pdf/10.1377/hlthaff.19.6.132.

[5] *See* Manatt White Paper at pp. 17–27.

[6] Boulding, M. "Self-Regulation: Who Needs It?," Health Affairs, Volume 19, Number 6 (2000), available at https://www.healthaffairs.org/doi/pdf/10.1377/hlthaff.19.6.132.

Program Goals

The goal of the program envisioned by our framework is that compliance with the self-regulatory program would be viewed by consumers as a "Good Housekeeping Seal of Approval," i.e., the gold standard for privacy-protecting technology. Through widespread promotion and adoption, certification of technology products through the program would ultimately become the industry standard.

Key tenets of the proposal are strong accountability and enforcement mechanisms, including comprehensive audits, spot checks and annual assessments, all of which would complement existing government regulation through the FTC.[7] The program would act as a partner to FTC regulators and state attorneys general (AGs) in that it would offer its participants compliance resources that government authorities may not have, such as time, infrastructure, and industry expertise.[8] This program would offer widespread monitoring and, given the already stretched resources of the FTC in particular, allow the commission to focus its efforts against the most egregious violators.

Establishment of a New Self-Regulatory Program

Operationalizing a new self-regulatory program will take extensive planning. Discussions about who might house a program of this type have centered around how the program should function rather than who should manage it. Although no final recommendations about program ownership were determined, several related issues were identified as needing further exploration. These will be considered during the second phase of this work:

- Ideally, the program would be housed in an existing organization rather than stood up as a brand-new entity. Succeeding at the latter would require more resources and a significantly heavier lift in terms of establishing name recognition and figuring out program logistics and a management structure. A number of reputable organizations have experience running self-regulatory programs in other industries.
- An organization that has a road map in place with experienced personnel to implement the new program would also lend credibility to the entire program for both consumers and regulators. There may be a need for an advisory body as part of the governance structure, another area for determination at a later date.
- A funding mechanism. Although funding details are for a later phase of work, the intention is that participating entities would pay an annual fee, scaled based on their size in terms of gross revenue.
- A sound economic model is key to a successful program, and in the implementation phase of this work, significant time and attention would be devoted to related logistics and ensuring that there are no conflicts of interest, whether real or perceived.

[7] While the Office for Civil Rights within the Department of Health & Human Services is the compliance and enforcement body for HIPAA-covered entities, it is the FTC that has similar authority for businesses outside HIPAA, even if they collect and use health data.

[8] *See* Manatt White Paper at p. 22.

Consumer and Participant Benefits

An inherent tension exists between "carrots" and "sticks" for encouraging and driving participation in the proposed program. Shoring up protections for consumers, as well as providing accountability and enforcement mechanisms, were the key areas this proposal sought to address. Consumers are often skeptical of self-regulation in the healthcare space due to perceived bias among participating companies. The introduction of a third-party, independent monitoring entity, with the backstop of FTC enforcement, would help assuage those worries.

During the next phase of this work, we will devote significant time and effort to involving consumers and consumer advocacy groups in fleshing out how this program will be implemented. Addressing consumer skepticism head-on by engaging consumer groups in these discussions will be critical.

To ensure the success of this program, participating entities will need meaningful incentives to join. The program will provide participants a way to distinguish themselves in an increasingly competitive market marked by widespread consumer distrust. And this benefit is real: Cisco's 2020 Data Privacy Benchmark Study, drawing from data from 2,800 organizations in 13 countries, showed that 70 percent of organizations say they received significant business benefits from privacy beyond compliance—up from 40 percent in 2019.[9] Further, "82 percent of organizations see privacy certifications as a buying factor: Privacy certifications ... are becoming an important buying factor when selecting a third-party vendor."[10]

As noted in the Executive Summary above, this framework creates a potential road map for future data privacy legislation. Companies that join as participants thus have the potential to be "ahead of the curve" when adopting the framework's policies. The combination of this with reputational and commercial benefits should provide significant incentives for companies to join.

Incorporation of Feedback

We received a number of thoughtful and detailed comments from a variety of stakeholders on all aspects of this framework, including the proposed self-regulatory structure. The above strives to address the majority of these, as do the adjustments to the following proposal. The most significant change to the draft released in August is the explicit recommendation that this new program be housed in an existing entity rather than established as a brand-new, stand-alone organization. As articulated above, we believe this will put us in a much stronger position for eventual implementation as well as help address many of the logistical and reputational questions we received. Perhaps most important, a reputable umbrella organization would help our program achieve far greater stakeholder confidence and trust, ultimately making it more meaningful for consumers and more attractive to potential participants.

[9] "Cisco 2020 Data Privacy Benchmark Study Confirms Positive Financial Benefits of Strong Corporate Data Privacy Practices," available at https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=2047256&utm_source=newsroom.cisco.com&utm_campaign=Release_2047256&utm_medium=RSS.

[10] *Id.*

Self-Regulatory Program for Non-HIPAA Healthcare Data

The proposed framework structure is a self-regulatory program focused on accountability: an independent, self-certification model designed to hold participating entities to a set of standards separately developed through a multistakeholder process. The program, housed in and run by an independent nonprofit organization, would accept individual companies as participants. Participating entities would submit their products for certification and individual products validated as compliant with the framework would be certified.[11]

Participating entities would undergo a thorough onboarding review at enrollment, be educated as to the self-regulatory framework and its obligations, publicly commit to complying with it, and submit to annual audits and assessments. Additionally, active spot-check monitoring would be done on a random sample of participants throughout each year. Participating entities could publicly market their participation and certification level as an "XXX Health Data Privacy Participant" (name TBD) and receive a recognizable visual certification symbol to mark them as such.

Participant fees would be collected from participating organizations to maintain the program. The amount of the fee would be on a sliding scale, based on the size of the company in terms of gross sales. Annual fees would also depend on the amount of seed money put forward to stand up the program at its origination.

Relevant components of this program would include:

- Rigorous onboarding, including the submission of a detailed questionnaire regarding business practices to ensure compliance with program standards;
- Annual audits and compliance assessments;
- Ongoing monitoring of participant companies, including random spot checks;
- Criteria to ensure that the reviews and assessments conducted by the program are independent of the 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, requirements, and governance logistics; listing participating covered organizations; and providing a simple and straightforward method for consumers to ask questions and file complaints about any product and/or any participating covered organization;

[11] Included entities will be all companies that collect, use or process health-related personal data. These would include, among others: hardware manufacturers; app developers; website publishers; third-party data management, brokering, collection or use outfits; and, potentially, businesses/employers that rely on third-party health technology in order to maintain the health of their workers.

- A standardized set of privacy rules that includes:
  - A broad, use-based definition of consumer health information;
  - Articulated appropriate uses and obligations surrounding the collection and use of consumer health information;
  - Greater consumer access to and control of their health information; and
  - Clear notice and transparency requirements; and
- An annual report card by program staff, publicly released, detailing the program's activities and effectiveness during the preceding year in obtaining compliance by participating covered organizations and in taking meaningful disciplinary and corrective actions for noncompliance.

Accountability and potential enforcement mechanisms for participating entities would include:

- Independent monitoring by program staff or other authorized evaluators, including publicly announced corrective or disciplinary cases;
- An active complaint-gathering process, clearly articulated in all public-facing materials and websites;
- A dispute resolution mechanism for resolving consumer complaints or complaints by another company based on the program's standards, and potentially providing consumers with redress for violations;
- A requirement to develop a corrective action plan (CAP) in the event of noncompliance and a process to lose certification if the CAP fails;
- Public announcement of investigations into complaints and complaint resolution, ensuring no complaints are ignored;
- Penalties for persistent or willful noncompliance 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; and
- Potential for FTC and/or state AG enforcement of violations of agreed-to standards.

This type of self-certification program would help level the playing field among businesses, fostering a unified set of privacy practices that are responsive to recent regulation. At the same time, it would raise 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 easily be converted into a safe harbor-style accountability mechanism in future legislation, giving it lasting utility even should new laws be passed.

Appendix

Steering Committee Members

The following organizations and individuals are some of those who participated in the development of this framework by virtue of being part of our Steering Committee. This committee met twice, in February and July of 2020, and many members also participated in one of our workgroups and/or offered feedback on earlier drafts of these proposals. Participation in the Steering Committee does not signify an endorsement of this framework, either in whole or in part. Rather, our Steering Committee provided valuable counsel and constructive criticism over the course of the framework's development. This final product reflects the work of the Center for Democracy & Technology and Executives for Health Innovation alone.

Joseph Ashkouti
Change Healthcare

Jacqueline Baratian
Ascension Health

Julie Barnes
Maverick Health Policy

Robert Belfort
Manatt

William Bernstein
Manatt

Melissa Bianchi
Hogan Lovells

Susan Bouregy
Yale University

David Brody
Lawyers' Committee for Civil Rights Under Law

Rebecca Cady
Children's National Hospital

Shawneequa Callier
George Washington University

Joanne Charles
Microsoft

Henry Claypool
American Association of People with Disabilities Consultant

Andy Coravos
Elektra Labs

Corey Cutter
American Cancer Society

Paul Eddy
Wellmark

Mary Engle
BBB National Programs

Shari Erickson
American College of Physicians

Dani Gillespie
National Partnership for Women & Families

Tina Grande
Healthcare Leadership Council

Carlos Gutierrez
LGBT Technology Partnership & Institute

Rachele Hendricks-Sturrup
Future of Privacy Forum

Laura Hoffman
American Medical Association

Alice Jacobs, M.D.
Convergence Group

Sean Kennedy
Salesforce

Jeri Koester
Marshfield Clinic Health System

Erin Mackay
National Partnership for Women & Families

Amy McDonough
Fitbit

Meg McElroy
Ascension Health

Deven McGraw
Ciitizen

Dena Mendelsohn
Elektra Labs

Ben Moscovitch
The Pew Charitable Trusts

Brenda Pawlak
Manatt

Jules Polonetsky
Future of Privacy Forum

Jessica Rich
Institute for Technology Law and Policy at Georgetown University Law Center

Alejandro Roark
Hispanic Technology & Telecommunications Partnership

Rajeev Ronanki
Anthem, Inc.

Alaap Shaw
Epstein Becker Green

Ashley Thompson
American Hospital Association

Lee Tien
Electronic Frontier Foundation

Charlotte Tschider
Loyola University Chicago School of Law

Nicol Turner-Lee
Brookings Institution

Ann Waldo
Waldo Law Offices

Marcy Wilder
Hogan Lovells

Po Yi
Manatt

Ashwini Zenooz
Salesforce

FOR MORE INFORMATION, PLEASE CONTACT:

Center for Democracy & Technology
CDT.ORG

Andrew Crawford
Policy Counsel
acrawford@cdt.org

Executives for Health Innovation
EHIDC.ORG

Alice B. Leiter
Vice President and Senior Counsel
alice@ehidc.org

CENTER FOR DEMOCRACY & TECHNOLOGY

EXECUTIVES FOR HEALTH INNOVATION