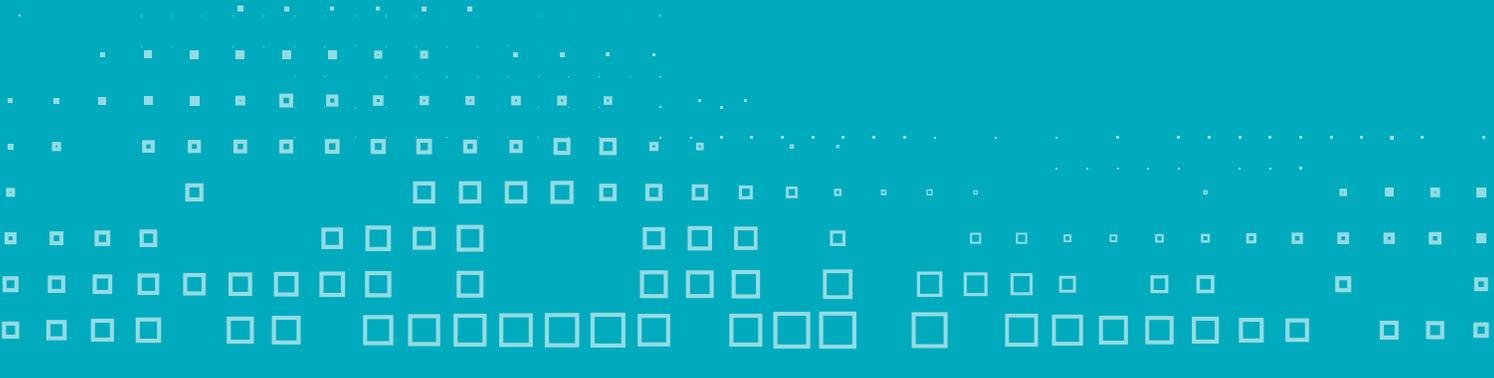


JUNE 2020

# **A Shared Responsibility: Protecting Consumer Health Data Privacy in an Increasingly Connected World**

**Robert Belfort**, Partner  
**William S. Bernstein**, Partner  
**Alex Dworkowitz**, Partner  
**Brenda Pawlak**, Managing Director  
**Po Yi**, Partner



## About The Robert Wood Johnson Foundation

For more than 45 years the Robert Wood Johnson Foundation has worked to improve health and health care. The Robert Wood Johnson Foundation is working alongside others to build a national Culture of Health that provides everyone in America a fair and just opportunity for health and well-being. For more information, visit [www.rwjf.org](http://www.rwjf.org). Follow the Foundation on Twitter at <https://twitter.com/rwjf> or on Facebook at <https://www.facebook.com/RobertWoodJohnsonFoundation>.

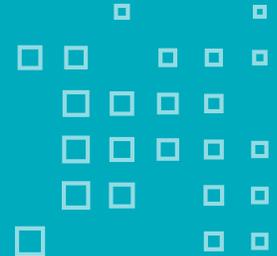
## About Manatt Health

Manatt Health integrates legal and consulting services to better meet the complex needs of clients across the healthcare system.

Combining legal excellence, firsthand experience in shaping public policy, sophisticated strategy insight and deep analytic capabilities, Manatt Health provides uniquely valuable professional services to the full range of health industry players.

Manatt Health's diverse team of more than 160 attorneys and consultants from Manatt, Phelps & Phillips, LLP, and its consulting subsidiary, Manatt Health Strategies, LLC, is passionate about helping our clients advance their business interests, fulfill their missions and lead healthcare into the future. For more information, visit <https://www.manatt.com/Health>.

# A Shared Responsibility: Protecting Consumer Health Data Privacy in an Increasingly Connected World



## Table of Contents

I.	Introduction .....	5
II.	Legal Landscape: Current Laws Provide Little Protection for Many Types of Health Data .....	7
III.	The Imperative for Action .....	11
IV.	Developing an Effective Consumer Privacy Framework for Health Data .....	14
V.	A Deeper Dive on Self-Regulatory Options: Overview of Relevant Models and Lessons Learned From Other Industries .....	19
VI.	Possible Self-Regulatory Options for Health Data .....	24
VII.	Considerations for Developing a Privacy Framework for Health Data .....	27
VIII.	Appendix .....	28

Dear Reader:

This paper was completed prior to the life changing events of the global COVID-19 pandemic. The world has changed in both salient and subtle ways that none of us could have predicted just a few months ago.

Over the coming weeks and months, patients, policymakers, healthcare providers and technology companies alike will have to grapple with challenging questions related to the power and promise of—but also the potential for harm from—digital technologies to support public health efforts to manage and contain the spread of lethal viruses, to quickly identify and provide targeted, vital supports for those affected, especially our most vulnerable residents, to support efforts to address health disparities, and to support efforts to safely resume much needed but delayed medical care, reopen our economy and resume our daily lives. The same digital exchange and aggregation of identifiable consumer data coupled with sensitive health information that can do so much for the greater public good can also have devastating consequences for individual lives if not afforded adequate privacy and security safeguards.

The COVID-19 pandemic puts the immense value of interoperable health data—across healthcare providers, insurance plans, settings of care, and patients—squarely in the spotlight. Indeed, in just early March, the federal government released its regulations to promote greater data liquidity and prevent “information blocking” amongst data stewards and technology vendors. The concept behind these rules is to more quickly, easily and without artificial barriers get patients’ own health information into their hands via digital app-based technologies and to ensure exchange of more data across health plans and care givers. But these rules did not extend privacy protections to patient data once released to technology developers and app vendors, instead relying on the market and general consumer protection laws.

The premise of this paper is that while more comprehensive federal privacy regulations are a worthy goal and may come in the future, alternate or additional paths for setting and enforcing strong privacy protections should be considered in parallel to protect consumer privacy related to their health data, including review of efforts from other industries. The health data industry is changing so rapidly and available electronic data pertaining to an individual’s health status is growing at such an exponential pace, the lengthy and complex legislative process cannot keep up with the increasingly critical need to have strong and comprehensive consumer privacy protection for health data. The failure to do so will likely result in a complex patchwork of competing state-level regulations that will be difficult if not impossible to comply with or enforce...or worse.

While this paper does not directly focus on the new data privacy questions that continue to arise due to the pandemic, we believe the issues, considerations and questions it raises are all the more salient today and that the imperative to advance a meaningful consumer data privacy framework is more critical than ever.

## I. Introduction

As this decade begins, Americans are increasingly apprehensive about the privacy of their personal information. A recent survey found that approximately 4 out of 5 Americans are concerned about how their data is used, think the risks of companies' collection of their data outweigh the benefits and believe they have little control of their data.<sup>1</sup>

Nowhere is this issue more important than in regard to health data, a type of information that can contain extremely personal details about an individual. Enacted in 1996, the Health Insurance Portability and Accountability Act (HIPAA) is the primary law that protects health data in the United States. But HIPAA was adopted in a world where most health data was held either by or on behalf of traditional healthcare providers or health plans.

Today, companies that operate mobile apps, search engines, social media platforms and health-oriented websites have more health information about many of their users than a hospital has about most of its patients. Yet these technology companies typically are not subject to HIPAA or other health privacy laws. The amount of health information held by these companies continues to increase in volume and importance by the day.

In fact, new federal regulations, released in March and published in the Federal Register on May 1, 2020, will be a catalyst for unprecedented interoperability between patient medical records and health insurance claims information and consumer-oriented digital technologies, blurring the lines—along with consumer understanding—between when health data is protected under HIPAA and when it is not. These regulations and other government initiatives will require health plans and healthcare providers to make health data available to individuals through apps that generally fall outside the scope of HIPAA regulation.

Without a framework to regulate the use and disclosure of such information, this data is at risk of misuse. Further, a lack of trust can cause consumers to take steps to block the sharing of their data, even when such disclosure is for legitimate purposes such as the receipt of sought-after services or the support of important public interest initiatives, such as medical research.

While greater liquidity of health data holds out the promise of tremendous public good, the potential for harm from exploitation of this data<sup>2</sup> is very high, as such data can be sensitive, can be potentially embarrassing, and can enable various types of discrimination. As ever-increasing amounts of health data are being collected, aggregated, sold and mined by Internet search engines, marketing agencies and commerce-oriented business ventures, it is critical for consumers to understand and have control over how their health data is used.

In spring 2019, with support from the Robert Wood Johnson Foundation (RWJF), Manatt convened a roundtable of health policy, provider and industry leaders focused on lessons learned in the ten years since the enactment of the Health Information Technology for Economic and Clinical Health (HITECH) Act. The roundtable also addressed what the government's role should be in facilitating health data liquidity to help improve medical care, lower costs and empower consumers. General agreement exists that HITECH did significantly advance the more widespread adoption of electronic medical records and lay a foundation

for easier exchange of information, but that patients often face impediments to gaining full access to their own health data. While healthcare data interoperability efforts have focused to date largely on provider and administrative services, health data liquidity is evolving to enable consumers to have greater access to and to be better stewards of their health data. This changing paradigm is creating new industry partnerships, including through development of standards-based application programming interfaces (APIs).

One outgrowth of the roundtable was a comment letter jointly authored by the six former national coordinators for health information technology submitted to the Office of the National Coordinator (ONC) and the Centers for Medicare & Medicaid Services (CMS) in support of then-proposed (now final, though with implementation delayed due to the COVID-19 pandemic) regulations to advance interoperability and promote consumer-facing APIs. The letter raised privacy as a critical issue that had to be addressed to support meaningful data exchange and called on policymakers and industry leaders to develop a consumer privacy framework in parallel with broader interoperability efforts.<sup>3</sup>

Given this context, with funding from RWJF, the Center for Democracy and Technology (CDT) and the eHealth Initiative (eHI) are jointly convening a Steering Committee of experts and leaders representing healthcare, technology, and advocacy groups and consumers to take proactive steps to protect the privacy of health data that falls outside the bounds of current health privacy laws. The Steering Committee aims to identify steps to advance a privacy framework that promotes accountability and transparency, provides meaningful protection to consumers with respect to the use of their health data, and creates a level playing field for companies that act responsibly with respect to protecting their users' data.

RWJF also engaged Manatt to research—and provide support for the Steering Committee in understanding—the gaps in existing health data privacy protections and the implications these gaps may have for industry data use and consumer privacy and to catalog potential options for developing and implementing a new framework governing the collection, use and disclosure of health data, including self-regulatory models that rely on public-private partnerships.

## II. Legal Landscape: Current Laws Provide Little Protection for Many Types of Health Data

### Health Privacy Laws Typically Do Not Apply to Organizations Outside the Healthcare System

Although HIPAA is the most far-reaching health privacy law in the United States, it covers only information created, received or maintained by or on behalf of healthcare providers and health plans. The HIPAA privacy rule applies to “protected health information” or “PHI” created or received by “covered entities,” which include health plans, most healthcare providers and healthcare clearinghouses (entities that help transmit data between health plans and healthcare providers).<sup>4</sup> This means that when patients upload data to health apps on their own, or when a patient generates data through a wearable device, that data typically is not subject to HIPAA.<sup>5</sup> Moreover, if a covered entity discloses PHI to a non-covered entity at the patient’s request or with the patient’s authorization, the information transmitted loses its status as PHI and the recipient—as a person who is not subject to HIPAA—does not need to comply with HIPAA in regard to such information.<sup>6</sup>

The HIPAA privacy rule sets forth several privacy protections important to patients, including limiting the circumstances under which PHI may be used or disclosed, giving patients a right to access their PHI, and granting patients a right to amend their PHI if it is inaccurate or incomplete (see Appendix for more details). The HIPAA security rule requires covered entities and their business associates to adopt administrative, physical and technical safeguards to protect electronic PHI.<sup>7</sup>

#### Business Associate Agreements

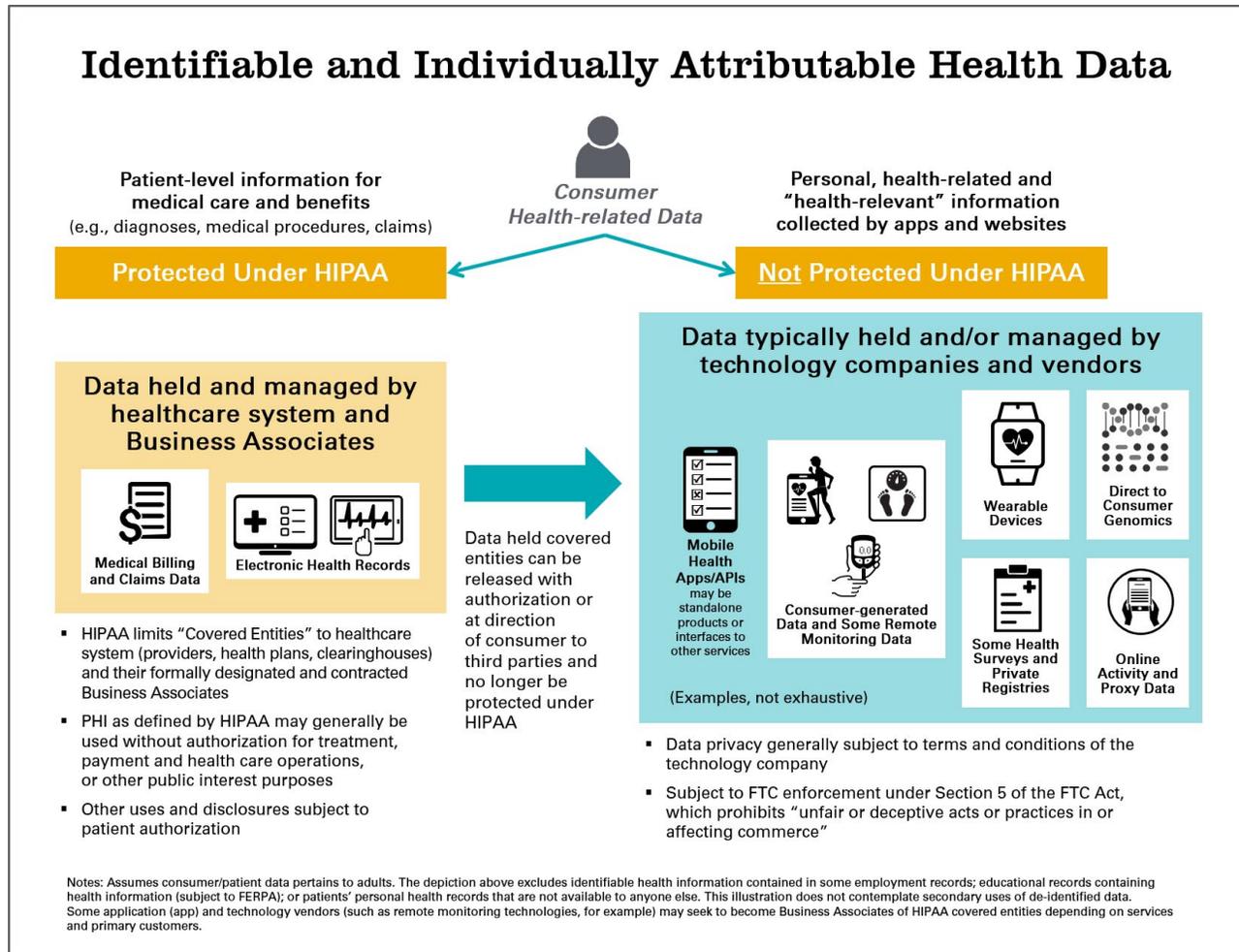
HIPAA does apply to one group of organizations outside of covered entities: contractors of such covered entities known as “business associates.” A technology company is a business associate of a covered entity if it creates, receives or maintains PHI on behalf of the covered entity, rather than under a direct relationship with the consumer. It is not always clear whether an app, wearable or other means of collecting health data is being made available to a consumer by a technology company in its own right or on behalf of a covered entity. The U.S. Department of Health and Human Services Office of Civil Rights has provided guidance on the factors that should be considered when evaluating whether a technology company is a business associate. In most cases, app developers and other technology vendors will not be business associates because they enter into direct relationships with consumers that do not run through covered entities. As a result, the health data they collect will generally not be treated as PHI that is subject to HIPAA.

See: <https://hipaaqsportal.hhs.gov/community-library/accounts/92/925889/Public/OCR-health-app-developer-scenarios-2-2016.pdf>.

Other health privacy laws also apply to healthcare providers and health plans but not technology companies. The federal substance use disorder confidentiality regulation, 42 C.F.R. Part 2, applies to certain healthcare providers that provide substance use disorder services.<sup>8</sup> The Family Educational Rights and Privacy Act (FERPA) applies to educational records from federally funded schools; this includes school health records maintained by such schools.<sup>9</sup> While states often have laws that protect the privacy of mental health information, information related to sexually transmitted diseases and other health information deemed sensitive, these laws typically apply only to healthcare providers and health plans, not technology companies. California's Confidentiality of Medical Information Act (CMIA), the state's equivalent to HIPAA, does apply to apps containing health information that is derived from providers of health plan records,<sup>10</sup> but the CMIA is the rare exception. HIPAA does not preempt more stringent state laws. As a result, there is a patchwork of state and federal health privacy requirements applicable to many providers and health plans.

## **The Use and Disclosure of Health Data Not Protected Under HIPAA Is Subject to Other Laws, but Those Laws Typically Are Narrower in Their Focus and Less Protective of Consumer Privacy Than HIPAA**

Section 5 of the Federal Trade Commission Act (FTC Act), which prohibits "unfair or deceptive acts or practices in or affecting commerce," is a national consumer protection statute that can be, and has been, used by the Federal Trade Commission to address the deceptive privacy practices of companies that operate outside of HIPAA. With its broad investigative and enforcement powers granted by the FTC Act, the FTC has been acting as the chief federal authority to protect the privacy of consumers' personal information, bringing numerous enforcement actions against companies for violating Section 5 of the FTC Act. A few actions in recent years have focused on health data, including an action against a technology company that solicited doctors' reviews from patients and publicly posted those reviews online without informing patients that the information they provided would be made public.<sup>11</sup> In addition, every state also has data breach notification laws. However, these laws focus on mandating that companies inform their customers if there has been a data breach involving their personal information and, in some cases, require these companies to provide free credit monitoring. Neither Section 5 of the FTC Act nor state breach notification laws are comprehensive privacy laws: They do not set forth the circumstances under which personal information may be disclosed, nor do they provide consumers with extensive rights in regard to their data.



The California Consumer Privacy Act (CCPA) is a comprehensive privacy law that is not limited to one industry and applies to many technology companies; the law provides consumers with multiple rights in regard to their data (see Appendix). The CCPA only applies to data on California residents held by for-profit businesses operating in California,<sup>12</sup> and it does not apply to any information that is subject to HIPAA. Other states, such as Illinois, New York and Washington, have considered laws similar to the CCPA, but so far, such bills have not passed state legislatures. Maine and Nevada have adopted statutes that impose certain privacy requirements on websites, and Illinois, Texas and Washington have adopted privacy laws for biometric information, but these laws are not as far-reaching as the CCPA.<sup>13</sup>

The General Data Protection Regulation (GDPR) of the European Union is a sweeping privacy law that affords consumers many of the same privacy rights under HIPAA and the CCPA, and it goes further than those laws in many respects. But the GDPR protects the data of American citizens only in limited cases.

Other countries, including Australia, Brazil, Japan, South Korea and Thailand, have enacted consumer data privacy rules; in some cases, these laws are modeled on the GDPR.

## New Federal Interoperability Rules Seek to Make Consumer Access to Health Data Easier but Do Not Address Privacy

In March 2020, ONC and CMS each announced final regulations to implement provisions in the 21st Century Cures Act<sup>14</sup> regarding the disclosure of data, but these rules aim to reduce barriers to the sharing of information and do not create a privacy framework. ONC's rule on information blocking prohibits healthcare providers, health information technology developers, health information exchanges and health information networks from interfering with, preventing or materially discouraging access, exchange or use of electronic health information, unless a specified exception applies.<sup>15</sup> This rule, for the first time, imposes sanctions on healthcare organizations for **failing** to share health data, rather than using or disclosing it improperly. A separate but related rule from CMS requires health plans that receive federal funding to implement and maintain an open API that permits apps, with the approval and at the direction of the consumer, to retrieve certain claims and clinical data maintained about the consumer by the plan.<sup>16</sup> The rule does not impose any new privacy restrictions on the further use or disclosure of such data once it is in an app and outside the scope of HIPAA regulation, relying on consumer decision-making and existing consumer protection laws and regulatory framework, such as under Section 5 of the FTC Act, as safeguards. In late April, CMS and ONC announced<sup>17</sup> short delays in the implementation-specific provisions in these rules and a temporary relaxation of enforcement of other provisions due to the COVID-19 pandemic, but both agencies signaled their commitment<sup>18</sup> to making it easier for consumers to access data and to advancing interoperability through implementation of these rules.

## Currently, No Clear Path to More Robust Consumer Health Information Privacy Protections

The current state of the law governing health data that falls outside the scope of HIPAA creates numerous challenges. It creates opportunities for the misuse of health data and substantial consumer harm, undermines trust in the collection and use of health data for legitimate and societally important purposes, subjects companies to a patchwork of state and federal laws with different requirements, and establishes a marketplace that makes it difficult for reputable companies to compete with less responsible data stewards.

The federal mandate to use standardized APIs for exchange of many types of medical and insurance data will revolutionize digital access to health data, which holds tremendous promise for the use of that data in improving care and empowering consumers. However, absent clear new privacy protections, responsibility for managing large stores of highly sensitive information falls almost exclusively to technology companies without clear lines of accountability.

Policy leaders, such as CDT, have encouraged Congress to enact a comprehensive federal privacy law, but the likelihood of such a law being adopted in the near future is not high. While other states may follow California by passing legislation modeled on the CCPA, those laws too will be geographically limited. Worse, these state privacy laws are unlikely to be harmonized, making compliance with privacy rules burdensome, even for companies dedicated to improving privacy protections.

## III. The Imperative for Action

### Health Data Not Subject to HIPAA Continues to Grow at a Tremendous Rate

As health data liquidity rapidly increases, the collection of this data has dramatically outpaced existing regulatory safeguards. One leading personal wellness wearables vendor (recently acquired by a global data, analytics and services company) has 28 million active users. Tens of millions of people have taken at-home genetic tests, providing their detailed genetic profiles to companies. Popular apps collecting health information—which includes information on sleep cycles, heart rates and periods—have millions of active users. And this pales in comparison to Internet search engines, which receive more than 1 billion health-related search questions every day.

The universe of patient health information generated from wearables, apps, search engines and other new technologies will continue to get bigger. According to some estimates, the global healthcare-related Internet of Things (IoT) market—including sensor-enabled wearables—is projected to reach \$534 billion by 2025, expanding at an annual rate of almost 20%.<sup>19</sup> Another recent analysis<sup>20</sup> predicts a 36% growth rate for health data over the next five years, a faster increase than in any other industry.

#### Uses of Data

The purposes for which a company uses data may relate in varying degrees to the purpose for which it collects (and in many cases monetizes) the data:

- Direct service or product delivery
- Analytics and product improvement
- New product or new service development (including development and use of machine learning, predictive analytics and AI)
- To target third-party advertising on a company's app, site or platform
- Data sold to third parties

### FHIR-Based APIs Are a Catalyst for the Health Data App Economy

The growth in consumer-generated health information is being matched by another form of health information not protected by HIPAA: information that was formerly PHI but has lost its protected status after being disclosed to a healthcare app at the consumer's direction.<sup>21</sup>

As noted above, the migration of PHI outside of the HIPAA-regulated environment is expected to accelerate rapidly once the new federal interoperability rules are implemented and requirements are in effect.<sup>22</sup> Since, under these rules, apps will be receiving PHI pursuant to a plan member's request to access to records, the apps will not be business associates of the health plans, and once the data is received by the app, they will no longer be subject to HIPAA. Hospitals and many physicians who participate in Medicare are already required to make patient data available on demand via APIs. Consumers requesting these transmissions may not be aware of this change in their data's legal status and the resulting reduction in privacy protection.

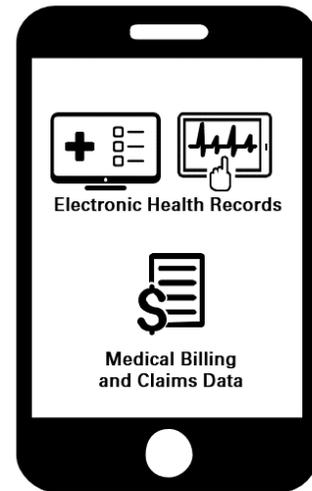
**Protected Under HIPAA**

**Data held and managed by  
healthcare system and  
Business Associates**



Consumer-directed  
release of data  
to an app  
  
Same data no longer  
subject to HIPAA  
protections in many  
cases\*

**Not Protected Under HIPAA**



**Mobile Health Apps/APIs**

\* The data may still be protected by HIPAA if a covered entity pays for the app, steers the consumer to the app, or directs the consumer to share data with the app.

While it is too early to accurately project the market size and economic impact of this shift, related industries have seen an explosion in the app economy. A conservative estimate valued the consumer-facing global app market at \$106 billion in 2018 and projects it will reach \$407 billion by 2026, with healthcare-related apps as one of the fastest-growing segments.<sup>23</sup>

However, privacy concerns are not just an abstract policy issue limited to consumers in an evolving mobile ecosystem. APIs are also currently used for a wide variety of business-to-business purposes, a market that will significantly increase as the universe of standardized data expands. Use of APIs for health data has significant implications for the ways major sectors of the economy—from healthcare providers to technology and device vendors to research institutions to pharmaceutical companies to retailers to health plans to governments, and many others—access and use data. Powerful business interests have a vested interest in how the health data API market evolves.

As adoption of APIs for clinical data by electronic health record (EHR) platforms, doctors, hospitals and health plans as well as a myriad of technology vendors increases, an individual patient's information will be increasingly "liquid" and more available on demand. This development holds tremendous promise for enhanced interoperability between disparate systems to share critically needed clinical information to improve care coordination, address gaps in care and enhance patient engagement. On the other hand, APIs will bring—indeed already are bringing—new entrants to the health data market, many of which are not accustomed to managing and protecting highly complex and sensitive health data.

## The Growth in Health Data Creates Privacy Challenges and May Undermine Consumer Trust

The proliferation of APIs is likely to have unintended consequences for patients (and their caregivers), who cannot be expected to understand that authorizing the release of their protected health information from a healthcare provider-managed system to a third-party mobile application vendor—possibly even one recommended by their doctor or hospital—may change the level of privacy protection, transparency and control they have over their deeply personal medical data.

As discussed in a 2019 report issued by the National Committee on Vital and Health Statistics (NCVHS), the construct of “protected health information” may be outliving its usefulness in a world of smartphones, tablets, wearable technologies, genetic testing services and web applications that collect data from the healthcare system at the direction of the consumer.<sup>24</sup> Consumers know that when they visit a doctor’s office, there are standards by which their information must be safeguarded, and that if a physician violates those standards, the physician may be subject to penalties. In contrast, when consumers provide the very same information—or in many cases, more detailed information—to a technology company that sells a wearable device or runs a search engine, there are few agreed-upon standards for the privacy of that information. Given that even personal data related to diet, exercise or purchasing habits has the potential to reveal sensitive information about an individual’s health status, this lack of both protection and transparency is hugely concerning from a consumer standpoint.

The lack of a common consumer privacy framework for health data in the brave new world, underpinned by clear regulatory guidance, creates serious challenges:

- **Trust:** Consumers lack trust in the companies that hold their health information.
- **Accountability:** Companies lack accountability to consumers in cases where they wrongfully use or disclose consumer health information.
- **Lack of awareness:** Consumers do not understand what privacy rights they have in regard to their health information.

One possible response is to let the status quo continue. But, as suggested above, there are many downsides of inaction. Consumer confusion and lack of trust will continue. Some states will follow California’s lead in adopting their own privacy laws, but those laws are likely to be inconsistent with one another, resulting in the worst of both worlds: a variation in standards across the country that fails to adequately protect consumers, and a host of new compliance responsibilities that increase the cost of doing business nationally. Companies that fail to take privacy seriously will continue to

A recent study published in the *Journal of the American Medical Association* (JAMA) found that apps frequently do not provide patients with clear terms of how their data will be used or disclosed and that 81% of the apps reviewed in their study transmitted data for advertising and marketing purposes or analytics to third parties.

See: Huckvale K, Torous J, Larsen ME. “Assessment of the Data Sharing and Privacy Practices of Smartphone Apps for Depression and Smoking Cessation.” *JAMA Netw Open*. 2019;2(4):e192542. doi:10.1001/jamanetworkopen.2019.2542.

function in a manner that puts consumers at risk, often without consequence, and companies that are more responsible data stewards will be at a competitive disadvantage in relation to these market participants. As a result, there is a clear imperative to develop a national privacy framework for health information.

### **The Role of Data Security Protections**

While the discussion in this paper primarily relates to developing a privacy framework for health data, robust, appropriate and effective data security protections must go hand-in-glove with any privacy approach.

Today, HIPAA-covered entities are required to implement appropriate administrative, physical and technical safeguards to ensure the confidentiality, integrity and availability of electronic protected health information. In addition, federally certified EHR technologies must demonstrate compliance with certain data security functionalities as a condition of certification. However, as discussed above related to privacy, these protections have limited application and exist largely within the confines of the traditional health system.

Health data security policies and functional solutions related to issues such as data storage, access, unauthorized use or disclosure, data breach, and loss or destruction of data, among others, must be advanced in parallel.

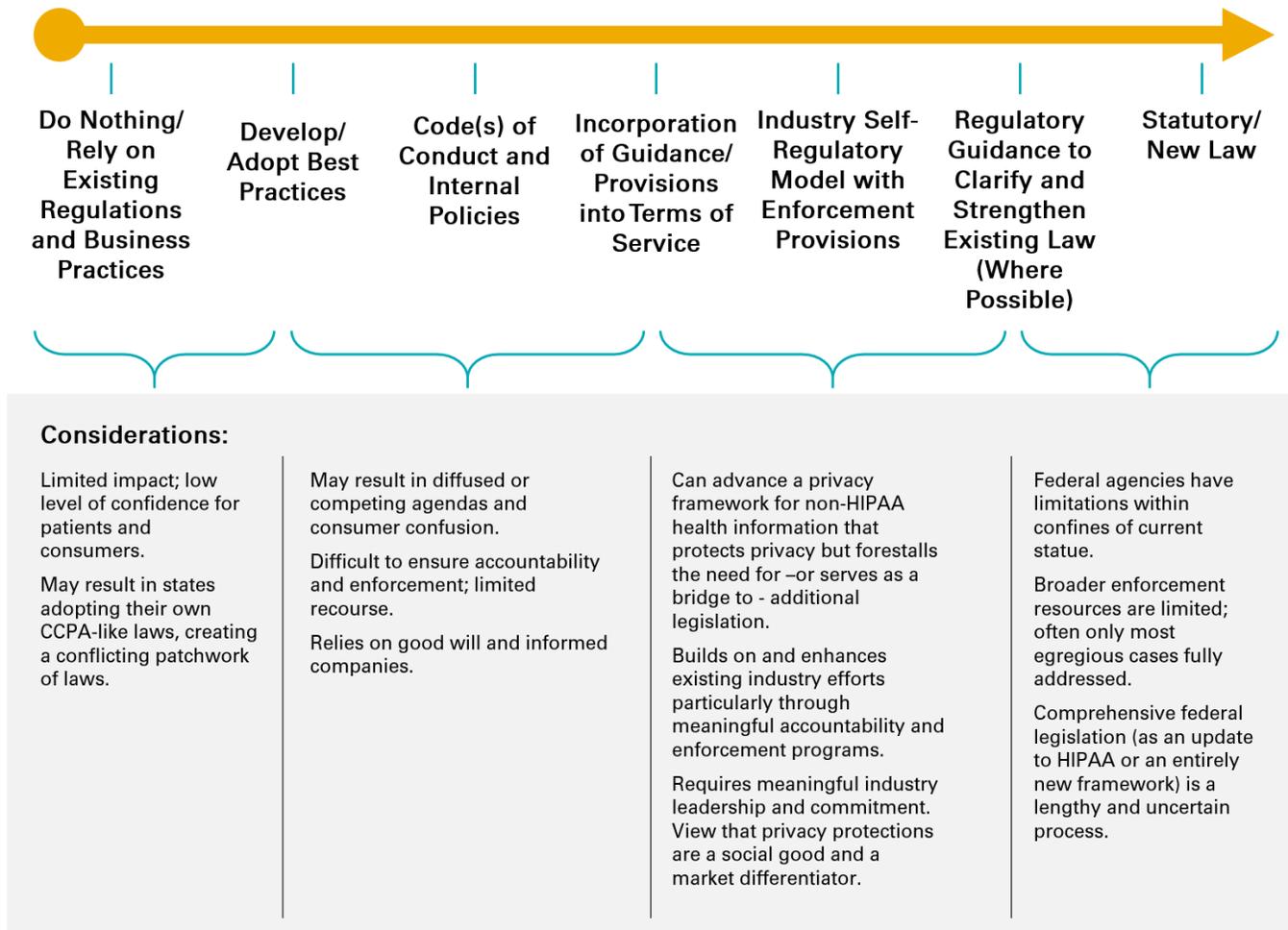
## **IV. Developing an Effective Consumer Privacy Framework for Health Data**

In the absence of a comprehensive federal privacy law, there is a critical need—and opportunity—for the private sector to adopt a new health privacy framework that provides accountability for the handling of health data that falls outside the bounds of HIPAA.

Such a framework must balance the interests of consumers in promoting industry accountability and transparency with the need for flexibility to foster innovation. By outlining clear pathways for how health data can appropriately be used to (i) improve patient health, (ii) enhance patient experience and (iii) reduce healthcare costs, a framework can provide flexibility while also protecting individual privacy.

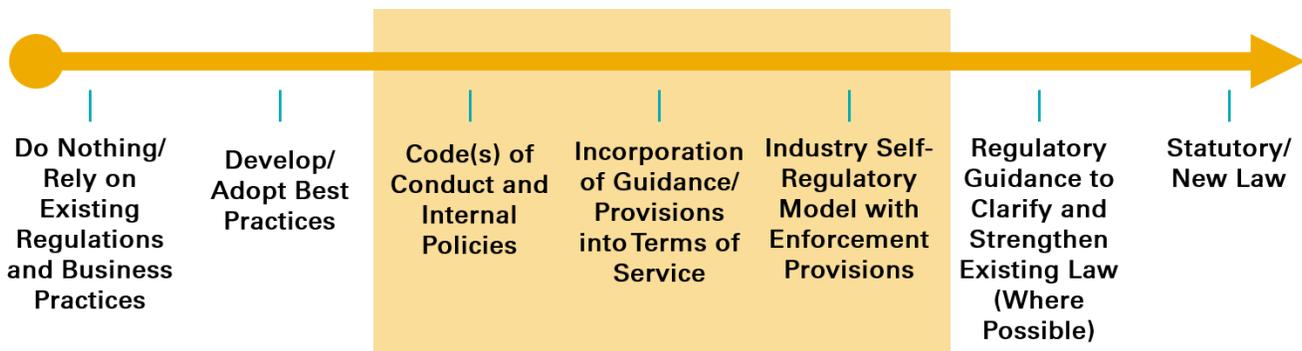
The visual below outlines a continuum of options for the Steering Committee to consider, some of which could be pursued simultaneously.

## Continuum of Consumer Health Data Privacy Model Options



Continuing a status quo approach and relying on market dynamics and existing business practices to underpin privacy protections is an untenable position, as public trust is low and state governments are increasingly stepping in, creating state-specific privacy regulations, which will create an exceedingly complex and challenging environment for businesses (and consumers) to navigate and ensure compliance. At the other end of the spectrum is enactment of sweeping new comprehensive federal privacy legislation. Many efforts to advance such legislation to date have stalled, and while the proliferation of state actions, recent high-profile cases of personal data misuse, and the growth of the app economy may add new urgency to the push for a new federal privacy law, the process remains lengthy and uncertain.

The Steering Committee has an opportunity to more rapidly advance a near-term solution or solutions, which may well be pursued in parallel with efforts to adopt more comprehensive federal legislative changes. These options fall in the “middle” of the continuum:



It is important to consider how these options might build upon and strengthen existing efforts from various stakeholder collaborations and existing laws to build a unifying framework, or at the very least, practical and effective pathways. It is also critical to understand that there are tradeoffs inherent in every approach.

## Codes of Conduct

Data privacy efforts, such as developing codes of conduct and adopting stringent company-specific privacy policies, may provide thoughtful and helpful guidance for companies. However, they are voluntary and have limited industry impact. It is rare today to find a company that does not have a privacy policy, but it can be difficult to ascertain whether such policies are actually meaningful to consumers, particularly because monitoring and enforcement are challenging.

Codes of conduct may be most effective when they apply to an industry sector or sub-sector, where the guidance and underlying use cases can be very specific. A code of conduct, such as one developed by an industry consortium or membership association, can be enforceable by the FTC or state attorney general offices if a company publicly pledges to adhere to it, though those agencies are limited by their available resources.

Significant efforts have been made across the past few years to convene multidisciplinary stakeholders and advance guiding principles and codes of conduct or guidelines related to data privacy protections, including (potentially among others):

- **The CARIN Trust Framework and Code of Conduct (May 2019):** The CARIN Alliance,<sup>25</sup> a multi-sector group of healthcare and other stakeholders, developed a voluntary code of conduct for entities not covered by HIPAA, such as third-party applications, when handling healthcare data accessed via APIs. The code includes provisions on transparency, consent, use and disclosure, individual access, security, provenance, accountability, education and advocacy.

- **Xcertia mHealth App Guidelines (August 2019):** Xcertia,<sup>26</sup> a mobile health app collaboration of over 40 organizations founded by American Medical Association (AMA), American Heart Association, DHX Group and Health Information Management Systems Society (HIMSS), developed a set of guidelines to promote clinician and patient trust in data privacy specific to emerging app technology. The guidelines include provisions on notice of use and disclosure; retention and access mechanisms; compliance with HIPAA, the Children’s Online Privacy Protection Act (COPPA), and GDPR; security; content; and usability.
- **Consumer Technology Association’s Guiding Principles For The Privacy Of Personal Health And Wellness Information (September 2019):** CTA<sup>27</sup> is a standards and trade organization representing more than 2,200 consumer technology companies in the United States. CTA drafted the principles to help its members address tangible privacy risks and securely collect, use, and share health and wellness data from health/wellness apps, wearable devices and other digital tools. The guidelines are based on five overarching principles: (1) Being open and transparent about how health and wellness information is collected and used; (2) being careful about how personal health information is used; (3) giving consumers control over the uses and sharing of their health information; (4) implementing strong security to protect health data; and (5) being accountable for practices and promises.

As an initial step, the Steering Committee should review these existing efforts to understand key areas of agreement and disagreement among these groups.

## Terms of Service

Companies may also incorporate privacy protections into their terms of service. Companies that incorporate privacy guidelines or elements of industry codes of conduct into their terms of service documents may be seen as signaling a stronger commitment to their customers.

However, terms of service documents tend to be lengthy, legally dense and difficult for consumers to understand. They also, in reality, tend to be structured to protect the company rather than the consumer, and it is often difficult for a consumer to raise complaints or to seek remediation. Finally, terms of service documents are company-specific and “one-off.” They can act as a mechanism to advance a privacy framework but are likely not a solution in and of themselves.

## Industry Self-Regulation Model With Enforcement

Self-regulation can be defined as “a regulatory process whereby an industry-level organization (such as a trade association or a professional society), as opposed to a governmental- or firm-level organization, sets and enforces rules and standards relating to the conduct of firms in the industry.”<sup>28</sup>

Industry self-regulatory models can be effective, as they tend to be more nimble and flexible than government regulation, competitors are incentivized to monitor each other, consumers have accessible ways to lodge complaints, and a foundational element of the model is a neutral enforcement mechanism. On the other hand, self-regulatory models may not represent all industry constituents and consequently may be narrower in scope than desired, with limited transparency.

However, a self-regulatory approach is useful to consider, as it may help circumvent inefficient regulation from a growing patchwork of laws that inadvertently create barriers to innovation or to entry. The FTC has noted that “a well-constructed self-regulatory regime has advantages over government regulation. It conserves limited government resources and is more prompt and flexible than government regulation, given the substantial time required to complete an investigation or to adopt and enforce a regulation.”<sup>29</sup>

Self-regulatory systems have been developed and adopted in other industries and typically contain the following core elements:

- Clear guiding principles/code of conduct
  - Strong industry support and adoption
  - System for amending existing guidance and adopting new guidance
- Transparency regarding participation, guiding principles/code of conduct and enforcement
  - Transparency within industry participants
  - Transparency to the public
- Effective evaluation and monitoring
  - Strong governance and authority
  - Rigorous system of monitoring
  - Independent, impartial evaluation and/or validation
- Consequences for noncompliance, supported by a “legal backstop” to escalate any matters that are not resolved through the self-regulatory process
- Self-sustaining business model to fund operations and enforcement

While self-regulatory models have proven effective on their own or as a bridge to legislation, they are not without criticism. An industry-developed model may be subject to bias, and the reliance on industry funding may lead to conflicts of interest. Transparency is essential.

## V. A Deeper Dive on Self-Regulatory Options: Overview of Relevant Models and Lessons Learned From Other Industries

Many organizations have recently published insightful works on privacy guidelines, codes of conduct and the like as related to health data privacy, which are worthy of review. Less has been promulgated on how self-regulation models might apply to health data and what specific models from other industries may be applicable for consumer health data privacy protections. The next two sections of this paper focus specifically on the self-regulatory option, reviewing lessons from other industries and outlining model options the Steering Committee may consider for health data.

Government regulations, like HIPAA, often focus on a specific industry. Similarly, self-regulatory systems govern specific industries or industry sub-sectors. Existing self-regulatory approaches in the advertising and financial services industries offer guidance on designing a self-regulatory system for health data and highlight effective system design and enforcement mechanisms (see Appendix for further details).

### Advertising Industry

Leading national advertising and marketing trade associations, including BBB National Programs,<sup>30</sup> the Association of National Advertisers (ANA), the Interactive Advertising Bureau (IAB), and the Network Advertising Initiative (NAI), represent different constituencies within the larger advertising industry ecosystem and often come together to implement cross-industry, independently enforced self-regulation.

#### Digital Advertising Alliance

The Digital Advertising Alliance (DAA) is an independent nonprofit organization led by leading advertising and trade organizations that establishes and enforces responsible privacy practices for online and mobile digital advertising while giving consumers information and control over the types of digital advertising they receive. The DAA was established in response to the FTC's review of the collection of information about consumers' online activity to target ads or content to individuals.<sup>31</sup>

The DAA runs the YourAdChoices program, which enables brands to provide enhanced notices to consumers about their interest-based advertising (IBA) practices and enables consumers to opt out of their information being used for future interest-based advertisements. The DAA also publishes Self-Regulatory Principles ("DAA Principles"), which address changing technologies and business models around multi-site, mobile and cross-device data.

Enforcement of the DAA Principles extends beyond participating companies to cover every company using consumer data for IBA and other covered purposes under the DAA Principles. Compliance with the DAA Principles is independently enforced for all companies that participate in relevant digital advertising by BBB

National Programs' Accountability Program and the Direct Marketing Association (DMA), a division of the ANA. While the Accountability Program and the DMA are part of the DAA through their parent organizations, they act as independent adjudicating bodies to address complaints filed by consumers, competitors and other stakeholders as well as through their own monitoring. Compliance with the decisions issued by the Accountability Program and DMA are voluntary, but noncompliance usually results in a referral to the FTC for further action.

### **Network Advertising Initiative**

The NAI is a nonprofit membership organization that works with leaders in online advertising to craft policies that help ensure responsible data collection and use practices. The NAI publishes and periodically updates its code of conduct and creates opt-out technologies for consumers in order to maintain the value of online advertising while protecting consumer privacy.

The NAI is an active participant and member of the Board of Directors of the DAA. While the DAA Principles govern the entire digital advertising ecosystem, the NAI's code of conduct imposes obligations only and exclusively to its member organizations, which are principally online advertising networks. The NAI regularly monitors its members for compliance with the code of conduct. If a member has materially violated the code of conduct, the NAI may suspend or revoke membership, publicly name a company or violation, and/or refer the matter to the FTC.

### **National Advertising Division**

The National Advertising Division (NAD), which is a part of BBB National Programs, assesses a broad scope of advertising claims and is generally viewed as the "gold standard" of self-regulation. The NAD has an extremely high compliance rate, despite the fact that participation in the self-regulatory process as well as compliance with NAD decisions are voluntary, largely because noncompliant or nonparticipatory companies usually have their cases referred to the FTC.

While the NAD does not have a formal relationship with the FTC or any other government organization, the FTC has been a vocal supporter of the NAD and has generally pursued matters referred by the NAD. Where appropriate, NAD also refers matters to other government agencies, including the Food and Drug Administration (FDA) and the United States Department of Agriculture (USDA), and state attorneys general offices.

Another advertising-related self-regulatory model of note is the Children’s Food and Beverage Advertising Initiative (CFBAI), which is administered by BBB National Programs. A voluntary initiative launched in 2007 with 10 charter members to combat growing child obesity, CFBAI today has 19 members representing the country’s leading food and beverage companies that are responsible for most of the child-directed food advertising expenditures in the United States.

Participants sign individual pledges agreeing to comply with a set of core principles on food advertising to children under 12, and CFBAI oversees the participants’ compliance with their respective pledges. In addition to CFBAI’s routine review of participants’ advertising activities, each participant submits an annual self-assessment that provides detailed information on its compliance procedures, ads distributed in children’s media and advertising plans.

If CFBAI finds noncompliance from any participant, it will provide the company with notice and an opportunity to bring its conduct into compliance. Failure to comply with the company’s pledge or to respond to CFBAI’s oversight requests may result in dismissal from the self-regulatory program and/or referral to the relevant regulatory authority.

## Financial Services

The financial services industry is heavily regulated, in part by the Securities Act of 1933 and the Securities Exchange Act of 1934. These laws created the Securities and Exchange Commission (SEC) to protect individual investors and ensure that the securities markets operate fairly. In order to do so, the SEC has oversight over several other agencies. Aspects of the industry that are not governed by relevant laws are governed by standards set by major industry players.

Self-regulatory bodies in this industry often act as gatekeepers—i.e., adherence to self-regulatory standards established by governing bodies is required to engage in the industry. Thus, in addition to financial penalties and reputational harm, noncompliance serves as a complete barrier to entry.

### Financial Industry Regulatory Authority

Neither a true self-regulatory organization nor a government agency, the Financial Industry Regulatory Authority (FINRA) is an independent organization under the purview of the SEC. It writes and enforces the rules governing its members, exchange markets, registered brokers and broker-dealer firms in the United States. Despite having regulatory powers similar to those of the SEC, FINRA is not subject to the same mechanisms that hold other federal regulators accountable.

Over time, FINRA has expanded its regulatory reach and collected millions in membership fees and fines. FINRA can fine or ban brokers and broker-dealers that violate its rules. It can also refer fraud and insider trading cases to the SEC and other government agencies for prosecution. Thus, FINRA serves as a gatekeeper for brokers and broker-dealers, who can be barred from the industry for noncompliance with its regulations.

## Payment Card Industry Data Security Standard

The Payment Card Industry Data Security Standard (PCI DSS) is a global standard mandated by payment card brands on entities that store, process or transmit cardholder data. PCI DSS emerged from a collaboration of the five major payment card brands, which previously had their own independent cardholder data security programs.

The Payment Card Industry Security Standards Council (PCI SSC) is responsible for the development and management of PCI DSS, including the creation of common data security requirements for merchants and service providers as well as a certification program for certain types of vendors. Each card brand maintains an independent validation program that requires tiered levels of compliance based on risk and primarily relies on acquiring and issuing banks to enforce the requirements.<sup>32</sup> As such, each payment card brand serves as the gatekeeper within its own payment network for transactions that are run through the network.

## Lessons From the Self-Regulatory Programs in the Advertising and Financial Services Industries

The advertising and financial services industries, as well as regulators generally, consider the self-regulatory programs discussed above to be successful in promoting more responsible behavior by the industry players and complementing and supplementing existing legal and regulatory frameworks. There are several common themes emerging from the review of these self-regulatory approaches relating to system design, compliance and enforcement.

**Program goals.** The shape of a self-regulatory program is largely dependent on the program's goals. If the goal of a program is merely to distinguish the good actors from the bad actors, then the program can be limited to a small segment of the industry (e.g., the NAI model) without wide industry adoption. While such a program can have rigorous standards and compliance requirements, including strong enforcement of such standards and requirements within a narrowly defined industry group, the program's impact in the industry is limited. If, on the other hand, the program's goal is to truly regulate the broader industry (e.g., the NAD for advertising generally, DAA for IBA, or online behavioral advertising, and FINRA for the broker-dealer industry), then the program needs to have a strong enforcement component with accountability.

**Self-regulation as a complement to government regulation.** Self-regulatory programs can co-exist with and support government regulation. Some self-regulatory programs, like the DAA, are created to address a perceived need for greater clarity and standards than the existing laws provide, and as a shield to additional laws that might not be as effective as industry self-regulation. Others, like the NAD, act as a critical industry partner to existing governmental regulation and supplement the government's enforcement efforts based on existing laws. In both cases, self-regulatory programs offer resources that the government may not be able to provide, including time, infrastructure and industry expertise. This allows for the entire industry to be better monitored, instead of the government using its limited resources only to enforce against the most egregious bad actors. In order for self-regulation to work effectively with existing government regulation, it is important both for the self-regulatory programs to evolve and innovate based on changing legislative and regulatory actions and for the government regulators to provide public endorsement or support of self-regulation.

**Transparency.** Legitimacy and effectiveness of self-regulatory programs require transparency. A high degree of transparency in the self-regulatory process, including requirements or criteria for participation, guiding principles and/or code of conduct and any changes to such principles or code of conduct, and the program’s monitoring efforts and enforcement activities, is important to gain the trust and confidence of the public, the industry players and government regulators.

**Consensus-based standard setting.** The diverging interests of different constituents create inherent conflicts of interest when creating industrywide or cross-industry standards. In order to achieve widespread industry buy-in, principles may not be as robust as consumers, government regulators or other participants may desire. This is of particular concern for the governance of yet-to-be-realized technological advancements, where pressure to quickly address such advancements could lead to watered-down and porous standards in order to accommodate the concerns of disparate groups represented in the self-regulatory body without delaying the issuance of the standards. By contrast, a narrower, membership-based or contractually enforced model can create standards that are both broader and stricter than consensus-driven standards.

**Independent funding and impartial oversight.** Self-regulatory programs must have a sound economic model to support the operation of their compliance and enforcement programs. Funding generally comes from membership fees, publication fees, archive subscription fees, penalties and/or other paid activities.

Self-funding complicates the need for unbiased, independent evaluation and adjudication. Without an independent body monitoring and enforcing self-regulatory standards, there may be a perception of bias and a loss of public trust. For instance, certain industries have contended with “pay to play” certifications, where a standard-setting body grants certification to any company that pays for it and does not adequately vet the companies to ensure compliance. This creates a misimpression with consumers that a sufficiently high standard is being complied with. As programs must make money by providing self-regulatory services to fund ongoing operations and oversight, walls and procedures need to be put in place to avoid a conflict of interest.

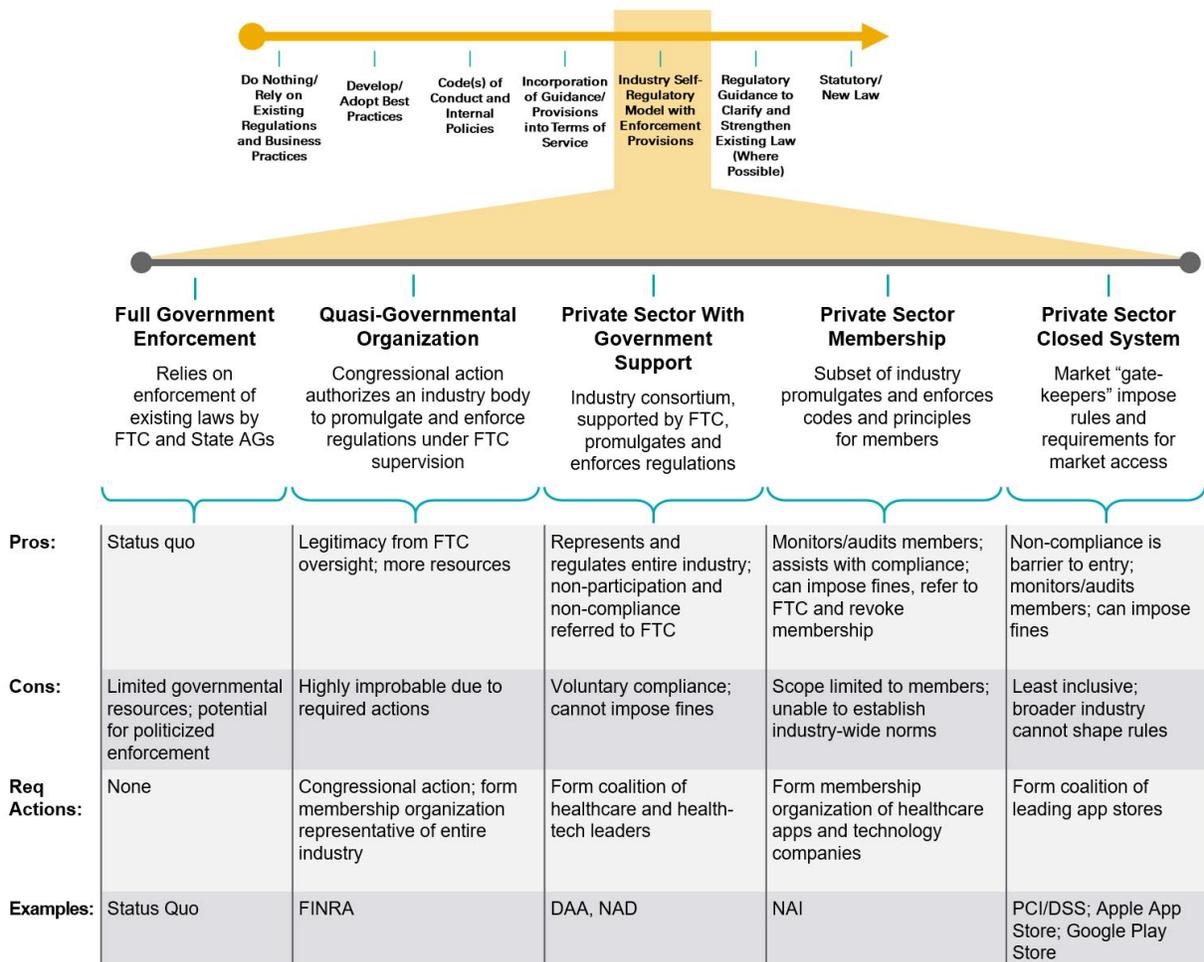
**Liability model vs. active enforcement.** A self-regulatory system can be enforced when industry leaders establish principles and contractually bind parties they directly contract with. In turn, those parties may pass this contractual obligation on to third parties that they directly contract with. In this instance, there may be several degrees of separation between those setting the standards and those following the standards. Monitoring and compliance efforts must be made by contracting parties in the middle. In practice, this risks becoming a liability model—i.e., liability for noncompliance is passed from one party to another. By contrast, a model with active enforcement is characterized by active oversight by an unbiased entity that is separate or wholly independent from the standard-setting body.

## VI. Possible Self-Regulatory Options for Health Data

There is not one path or blueprint for self-regulation. Rather, there are many approaches, ranging from industry players “co-regulating” with government entities to industry consortium oversight models to requirements for—or barriers to—market entry.

Within the category of “Industry Self-Regulatory Model” there are multiple model options that might be considered, and often more than one model may be pursued in harmony with others. The visual below outlines a continuum of potential options for enforcement and accountability based on our review of the existing models, which range from full government involvement to a closed, independent system.

### Multiple Self-Regulation Models



These models include:

- **Full Government Enforcement:** This model maintains the status quo, whereby the FTC and state attorneys general are solely responsible for enforcement. While this full government enforcement model can still allow for consumers and competitors to monitor the behavior of data collectors by submitting complaints directly to the agency, as is the case with HIPAA enforcement, limited governmental resources and political incentives will likely result in selective enforcement of only the most egregious cases.

No action is needed to follow this model. To the extent that additional privacy laws are enacted at the federal or state level, such additional laws will strengthen and sharpen the enforcement rights of the federal regulatory agency and state attorneys general offices, but they will not help mitigate the problem of limited governmental resources and potential for politicized enforcement.

- **Quasi-Governmental Organization:** Congress grants a private organization regulatory authority to promulgate guidelines and enforce standards for health data, with supervision by the FTC. This model is akin to the FINRA model employed in the broker-dealer industry, as well as the securities industry generally, where oversight by the SEC provides both legitimacy and resources.

To translate this model for health data, congressional action as well as the creation of a membership organization that is broad enough to include any company that handles health data would be needed.

- **Private Sector With Government Support:** A consortium of healthcare and health-tech leaders form a self-regulatory body, which operates independently from but in alignment with a federal regulatory agency, earning the support of the agency. This system would be modeled after the DAA and the NAD, whereby enforcement is handled by an independently funded adjudicatory body but is backstopped by the FTC. Unlike the prior options, enforcement is limited to adjudication on whether or not a company has violated the law or established industry standards. Enforcement is designed to offer recommendations to bring the company into compliance, with no power to actually require compliance or impose financial penalties. While compliance is voluntary, this model has succeeded in the advertising industry because nonparticipation and noncompliance with the adjudicating body's recommendations are referred to the appropriate federal regulatory agency or the state attorneys general.

This model could be employed for health data if a federal regulatory agency similarly endorses a new self-regulatory model. Self-enforcement, backstopped by the FTC, would incentivize the industry to promote more responsible actions under established principles and codes of conduct. Notably, these actions would create industrywide standards, as this model would regulate all entities that collect, use or otherwise process health data.

- **Private Sector Membership:** A consortium of healthcare apps and technology companies form a membership organization, which monitors its members and provides incentives for membership. This would be modeled after the NAI, as NAI membership has become the industry standard for online advertising networks and is often contractually required by advertisers. Because this is a membership-driven model, the consortium has broad enforcement powers, including the ability to impose fines. However, this model is limited in scope because enforcement extends only to members.

This model may be more practicable to employ, as only a subset of the industry using health data needs to form a membership organization. Incentives for membership may include certification that data is being handled responsibly and training for members on data use best practices. Adequate funding can be raised from membership dues and financial penalties. However, a membership organization would be unable to promulgate industrywide privacy practices for health data. This would not help harmonize the current landscape of varying and somewhat contradictory codes of conduct and best practices.

- **Private Sector Closed System:** App stores, serving as gatekeepers, control access to a closed system. This model is mirrored after PCI DSS, where each payment card brand serves as the gatekeeper within its own payment network for transactions that are run through the network. Notably, this model is even less inclusive than the previous option, as a smaller constituency is responsible for setting standards. However, it may result in the most effective enforcement, as noncompliance is a complete barrier to entry.

In the instant case, leading app stores could serve as gatekeepers if they agree to implement and enforce uniform review guidelines; app stores, including the Apple App Store and the Google Play Store, currently have individual review guidelines that can impose privacy-related requirements on hosted apps. If so, compliance with the uniform guidelines would be required to submit an app that uses, collects or otherwise processes health data. As access to the app stores is vital for the health technology industry, this model could result in very effective enforcement.

## A Related Approach: Accreditation or Certification

In addition to standards, codes of conduct, terms of service, and similar social and contractual controls, third-party accreditation and/or certification can be employed as tools under an industry self-regulatory model. Accreditation/certification can be incorporated into many structural models and approaches. To signal that a given product or company meets a set of standards (related to data stewardship practices, or to data privacy and security criteria, or to quality, for example), self-regulatory bodies may employ some form of voluntary accreditation or certification, which often includes an application or testing fee and ongoing attestation and/or monitoring of compliance. Accreditation/certification can signal to consumers that a given company or vendor has been vetted or tested using methodology that is approved by the relevant industry and deemed to meet a minimum threshold of standards or expectations established by the industry, and as such may display and market a “seal of approval.” Such programs may also be “tiered,” allowing companies to classify their products as having met different levels—in this case—of privacy and security controls (“bronze-, silver-, or gold-certified,” for example).

A successful accreditation or certification program requires a strong, trusted accrediting body and rigorous ongoing monitoring and audits as well as a process to revoke accreditation/certification from noncomplying companies.

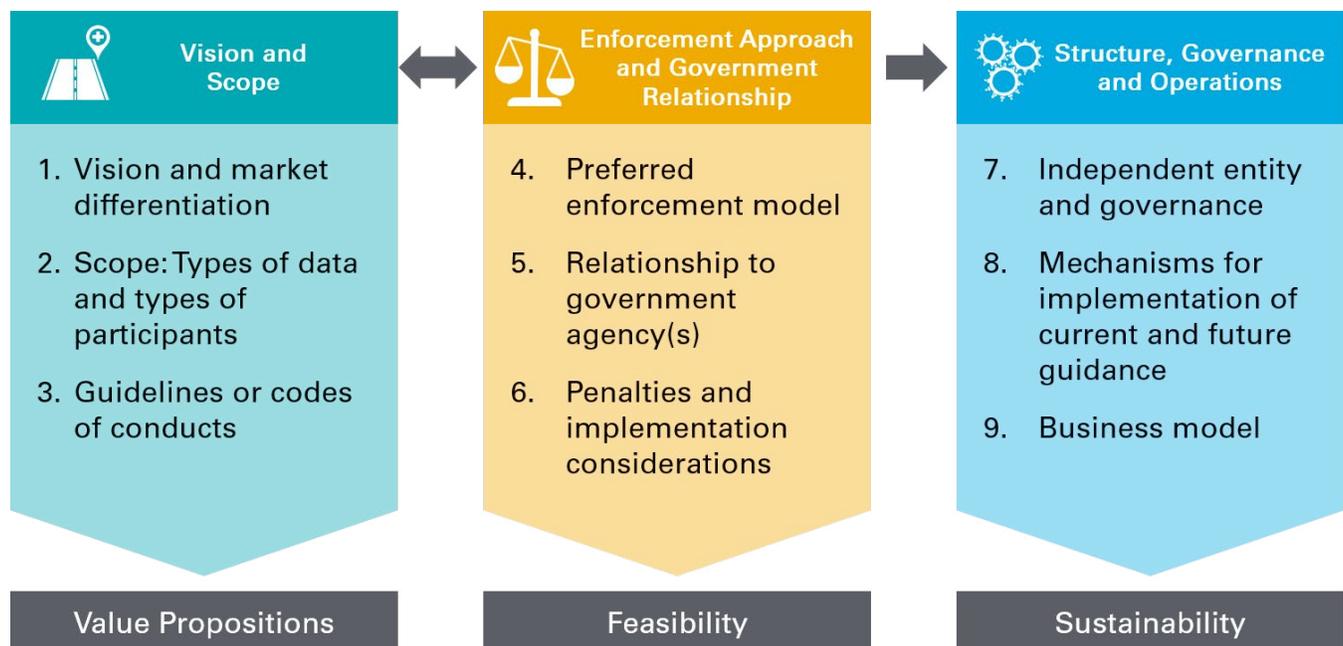
## VII. Considerations for Developing a Privacy Framework for Health Data

The work of the Steering Committee should consider the merits of various privacy framework pathways and how they might build upon and strengthen other industry efforts to become a positive competitive differentiator. In so doing, the Steering Committee can facilitate building the foundation of public and consumer trust that is critical to the transformational potential of digital technology in healthcare.

Over the coming months, we recommend the Steering Committee seek to develop consensus around the imperative for action and to define a vision and proposed initial scope for a privacy approach. This work will serve as the foundation for the development of a framework for how the model would advance and enforce privacy protections.

If a self-regulatory approach is determined to be a desirable model, future work will need to develop an operational approach including structure, scope of authority, governance, oversight and accountability mechanisms and processes, infrastructure requirements, and funding.

### Developing a Consumer Privacy Framework for Health Data



## VIII. Appendix

### Scope of Key Privacy Laws

HIPAA	CCPA	GDPR
<ul style="list-style-type: none"> <li>▪ Protected Health Information (PHI) held by covered entities and their business associates (contractors)</li> <li>▪ PHI: Information created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse:               <ul style="list-style-type: none"> <li>– Which relates to a physical mental health condition, the provision of healthcare, of payment for healthcare; and</li> <li>– Identifies an individual or could be used to identify an individual</li> </ul> </li> <li>▪ <b>Geographic focus:</b> Covered entities located in the US—healthcare providers, health plans, and healthcare clearinghouses</li> </ul>	<ul style="list-style-type: none"> <li>▪ Personal Information (PI) held by businesses and their service providers (contractors)</li> <li>▪ Personal Information: Information that identifies or is capable of being associated with a particular consumer or household. Excludes publicly available information</li> <li>▪ Businesses: For-profit organizations that either: (A) have annual revenues of more than \$25 million, (B) process PI of more than 50,000 consumers, or (C) derive more than 50% of revenue from selling PI. Non-profits/government organizations not subject to the CCPA.</li> <li>▪ CCPA does not apply to PHI under HIPAA or “medical information” under the California Confidentiality of Medical Information Act (State law equivalent of HIPAA)</li> <li>▪ <b>Geographic focus:</b> Only to businesses and residents in California</li> </ul>	<ul style="list-style-type: none"> <li>▪ Personal Data (PD) held by controllers and their processors (contractors)</li> <li>▪ Personal Data: Any information relating to an identified or identifiable natural person</li> <li>▪ Subcategories of Personal Data: Data concerning health, genetic data, biometric data</li> <li>▪ Provides strong rights to individuals, in addition to the right of consent, such as the right to erasure (otherwise known as the right to be forgotten) and rights to data portability</li> <li>▪ <b>Geographic focus:</b> Applies to U.S. businesses if they:               <ul style="list-style-type: none"> <li>– Establish presence in the EU (e.g., an EU office) and they process PD that relates to that established presence;</li> <li>– Offer goods or services in the EU;</li> <li>– Monitor behavior that takes place in the EU (e.g., cookies track online behavior on computers within the EU)</li> </ul> </li> </ul>
<p><b>FTC Act</b></p>	<ul style="list-style-type: none"> <li>▪ The Federal Trade Commission (FTC) has broad authority over consumer data by way of provisions in the FTC Act that prohibit “unfair or deceptive acts or practices.”</li> <li>▪ This prohibition applies to all entities engaged in commerce.</li> <li>▪ However, the FTC Act does not contain a set of substantive privacy standards</li> </ul>	

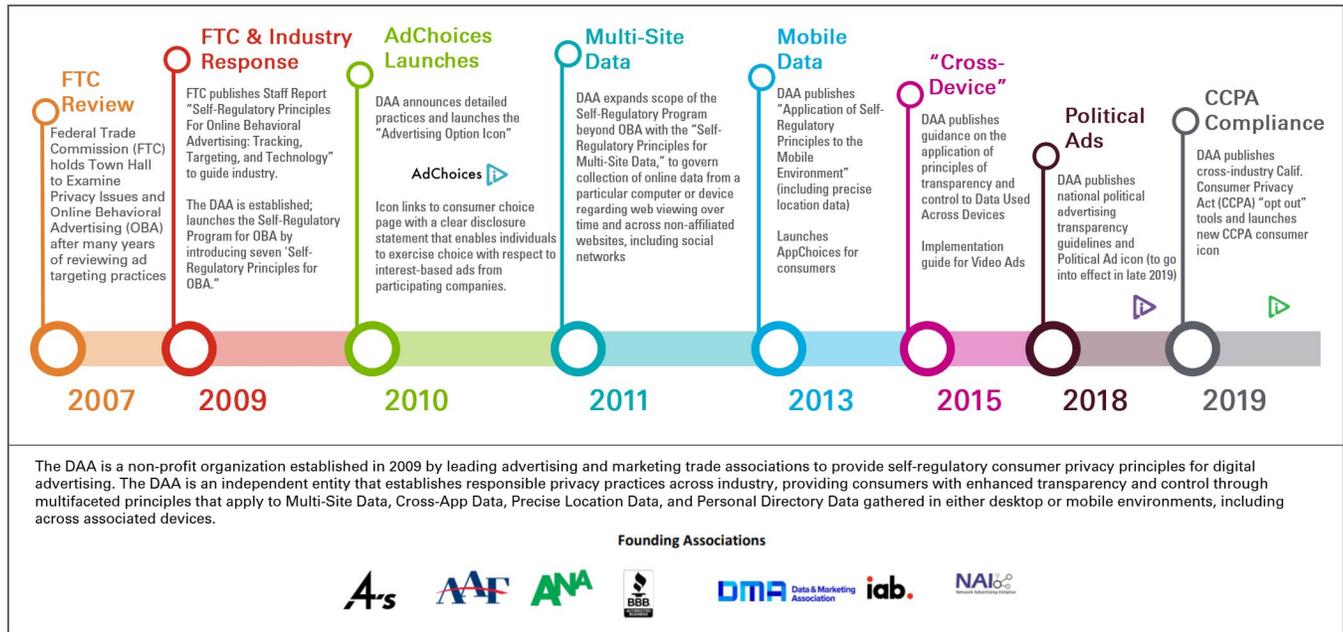
## Comparison of Privacy Protections: HIPAA, CCPA and GDPR

Issue	HIPAA	CCPA	GDPR
<b>Consent for disclosures required?</b>	Not needed if disclosure is for purposes of treatment, payment or health care operations, or limited other purposes	Only if disclosure involves a sale of a child's PI	Not needed if processing is lawful on another basis. Health data may be disclosed without consent if the purpose relates to treatment or the management of health or social care systems, among other reasons
<b>Sale of information permitted?</b>	No, unless undertaken pursuant to an authorization	Yes unless (1) consumer exercises opt-out right or (2) information relates to a child and there is no authorization	Yes, but individual may prohibit if disclosure is made for marketing purposes
<b>Breach notification required?</b>	Yes, if breach of unsecured PHI	No (addressed in other state law)	Yes, unless unlikely to result in a risk to rights or freedoms
<b>Notice on data practices required?</b>	Yes, must provide individuals with a notice of privacy practices describing potential uses and disclosure of PHI	Yes, must notify individuals re categories of personal information collected and purposes for which information is used	Yes, must provide notice regarding purposes for processing, retention periods, etc.
<b>Limitations on collection and use of data?</b>	Yes, minimum necessary standard applies, subject to exceptions	No	Yes, requires data to be minimized; includes principles of reasonableness, proportionality, necessity, and purpose limitations
<b>Right to prohibit disclosures?</b>	Only if info was disclosed to health care provider for emergency treatment	Only if information is sold	Yes, if PD is processed for marketing purposes or under other limited circumstances
<b>Right to access information?</b>	Yes, must provide within 30 days	Yes, must provide within 45 days	Yes, must provide within one month
<b>Right to data portability?</b>	Yes, must provide directed disclosure within 30 days	"Shadow" right: must provide information in a format that allows transfer without hindrance	Yes, must transfer data to another controller where technically feasible
<b>Right to amend information?</b>	Yes, if PHI is inaccurate	No	Yes, if PD is inaccurate or incomplete
<b>Right to delete information?</b>	No	Yes, subject to exceptions	Yes, under certain circumstances
<b>Right to accounting of disclosures?</b>	Yes, but doesn't apply to disclosures made with consent or for purposes of treatment, payment or health care operations	Yes	Yes
<b>Private right of action?</b>	No	Only for certain data breaches	Yes, individual has a right to file complaints/private actions and receive compensation

## Examples of Self-Regulatory Approaches in Other Industries

Advertising: DAA	
<p><b>Who is involved?</b></p> <ul style="list-style-type: none"> <li>Led by leading national advertising trade groups</li> </ul>  <ul style="list-style-type: none"> <li>Participants include brand advertisers, agencies, publishers, ad networks, and ad tech companies           <ul style="list-style-type: none"> <li>Over 150 AdChoices participants, including Google, Amazon, and Netflix</li> </ul> </li> </ul>	<p><b>What problem is being addressed?</b></p> <ul style="list-style-type: none"> <li>FTC recognized need to protect consumer privacy rights and tasked industry to develop program</li> <li>Cross-industry <b>self-regulatory principles</b> (DAA Principles) for online behavioral advertising (OBA) govern privacy practices for digital advertising</li> <li>AdChoices program allows advertisers to engage in OBA while giving consumers control over data collection and use via an opt-out mechanism</li> </ul>
<p><b>How does it work?</b></p> <ul style="list-style-type: none"> <li>Published 5 self-regulatory principles to-date addressing general OBA, multi-site, cross-device, mobile data and political ads           <ul style="list-style-type: none"> <li>Compliance is enforced by the BBB National Programs' Accountability Program and the DMA, a division of the ANA</li> <li>Complaints may be filed by consumers, business entities, or other stakeholders</li> </ul> </li> <li>Creates/manages various AdChoices icons; consumers opt-out of OBA by clicking the AdChoices icon</li> <li>Launched CCPA Opt-Out Tool in 2019</li> </ul> 	<p><b>What results have been achieved?</b></p> <ul style="list-style-type: none"> <li>A TRUSTe survey showed awareness of the AdChoices icon at 21% in 2014, 37% in 2015, and 42% in 2016</li> <li>The Accountability Program           <ul style="list-style-type: none"> <li>Publicly releases all decisions and administrative actions</li> <li>Released its 100th public action in 2019</li> <li>98% of actions result in full cooperation</li> <li>Non-cooperative companies were referred to government agencies</li> </ul> </li> <li>DMA           <ul style="list-style-type: none"> <li>Publicizes only non-compliant companies, but publishes an annual ethics compliance report</li> <li>From Jan. 2017 through July 2018, DMA               <ul style="list-style-type: none"> <li>Received 665 inquiries or complaints about digital advertising</li> <li>Referred 5 companies to government agencies, but not for violations of the DAA principles</li> </ul> </li> </ul> </li> </ul>

**Key Milestones—DAA’s Self-Regulatory Model**



Advertising: NAI	
<p><b>Who is involved?</b></p> <ul style="list-style-type: none"> <li>Over 100 participating ad networks engaged in IBA follow the NAI guidelines (Code of Conduct)                             <ul style="list-style-type: none"> <li>Members are listed on the NAI’s opt-out page</li> <li>Also listed as participants of the DAA and on the aboutads.info opt-out page</li> </ul> </li> <li>Consumers use opt-out tools to opt-out of IBA from NAI members</li> </ul>	<p><b>What problem is being addressed?</b></p> <ul style="list-style-type: none"> <li>While DAA focuses on brands, NAI focuses on vendors</li> <li>NAI Code of Conduct maintains the value of online advertising while protecting consumer privacy                             <ul style="list-style-type: none"> <li>Adopted in 2000 with the support and endorsement of the FTC</li> <li>Only binding on members</li> <li>Incorporates and expands on the DAA Principles</li> </ul> </li> </ul>
<p><b>How does it work?</b></p> <ul style="list-style-type: none"> <li>NAI enforces the Code of Conduct by:                             <ul style="list-style-type: none"> <li>Regularly monitoring members</li> <li>Responding to and investigating consumer complaints</li> </ul> </li> <li>For material violations of the Code of Conduct, NAI may:                             <ul style="list-style-type: none"> <li>Suspend or revoke membership</li> <li>Publicly name a company or violation</li> <li>Refer the matter to the FTC</li> </ul> </li> </ul>	<p><b>What results have been achieved?</b></p> <ul style="list-style-type: none"> <li>Many brands, agencies and publishers ask about NAI membership before partnering with ad tech companies</li> <li>NAI members are able to demonstrate commitment to data management practices</li> <li>The Code of Conduct is periodically revised to reflect new data uses and advertising needs. The 2020 code:                             <ul style="list-style-type: none"> <li>Includes digital advertising practices such as the use of offline data for tailored advertising</li> <li>Builds upon the required opt-in consent for the use of data about sensitive health conditions</li> <li>Incorporates elements of the CCPA</li> </ul> </li> </ul>

<b>Advertising: NAD</b>	
<p><b>Who is involved?</b></p> <ul style="list-style-type: none"> <li>• NAD is part of BBB National Programs, Inc.</li> <li>• Consumers, competitors, and local Better Business Bureaus can submit complaints</li> <li>• Advertisers voluntarily participate in NAD proceedings</li> </ul>	<p><b>What problem is being addressed?</b></p> <ul style="list-style-type: none"> <li>• Created in 1971 to increase public confidence in advertising</li> <li>• Ensures that cases are reviewed by experts in advertising law</li> <li>• Minimize government involvement in advertising by transparently settling competitor disputes</li> </ul>
<p><b>How does it work?</b></p> <ul style="list-style-type: none"> <li>• NAD reviews challenges against advertisers brought by third parties or initiates reviews based on its own monitoring program</li> <li>• Publicly reports formal decisions</li> <li>• Decisions are appealable to the National Advertising Review Board (NARB)</li> <li>• If a company does not to participate or comply, the case may be referred to the FTC</li> <li>• Introduced Fast-Track SWIFT (Single Well-defined Issue Fast Track) in 2020 to resolve matters with a single well-defined issue within 20 business days</li> </ul>	<p><b>What results have been achieved?</b></p> <ul style="list-style-type: none"> <li>• Handles about 150 cases each year about misleading and/or deceptive ads</li> <li>• 90+ percent compliance rate with more than 6000 decisions issued since its inception</li> <li>• FTC takes NAD referrals seriously and maintains an online database with resolutions of cases referred by NAD</li> </ul>

<b>Financial Services: FINRA</b>	
<p><b>Who is involved?</b></p> <ul style="list-style-type: none"> <li>• Overseen by the Securities Exchange Commission (SEC)</li> <li>• Registered brokers and broker-dealer firms in the U.S.               <ul style="list-style-type: none"> <li>– Including more than 3,700 brokerage firms, 155,000 branch offices, and 630,000 securities representatives</li> </ul> </li> </ul>	<p><b>What problem is being addressed?</b></p> <ul style="list-style-type: none"> <li>• Regulates the trading of equities, corporate bonds, securities futures, and options</li> <li>• Educates investors about unfair investment and trading practices to prevent fraud and mishandling of funds</li> </ul>
<p><b>How does it work?</b></p> <ul style="list-style-type: none"> <li>• Writes and enforces self-regulatory rules</li> <li>• Issues guidelines to help members understand and implement rules</li> <li>• Operates the largest securities dispute resolution forum</li> <li>• Maintains a searchable database of brokers, investment advisors, and financial advisors</li> <li>• Authorized by Congress to engage in certain regulatory work</li> </ul>	<p><b>What results have been achieved? (2019)</b></p> <ul style="list-style-type: none"> <li>• 591 disciplinary actions were filed against registered brokers and firms for unethical behavior</li> <li>• \$24 million was awarded in restitution to harmed investors</li> <li>• \$70 million total monetary sanctions (fines, restitution, and disgorgement)</li> <li>• In 2018, more than 900 fraud and insider trading cases were referred to the SEC and other agencies</li> </ul>

Financial Services: PCI DSS	
<p><b>Who is involved?</b></p> <ul style="list-style-type: none"> <li>• Managed by the <b>Payment Card Industry Security Standards Council (PCI SSC)</b></li> <li>• Arose from Visa and Mastercard’s security programs and endorsed by other card brands</li> <li>• Any business or organization that processes, stores or transmits cardholder data</li> </ul>	<p><b>What problem is being addressed?</b></p> <ul style="list-style-type: none"> <li>• Developed in response to impact and costs of payment card fraud and data breaches</li> <li>• Establishes a <b>uniform global standard</b> for storing, processing, and transmitting cardholder data</li> <li>• Previously, payment card brands each had different standards</li> </ul>
<p><b>How does it work?</b></p> <ul style="list-style-type: none"> <li>• Payment card brands determine requirements for validation <ul style="list-style-type: none"> <li>– Requirements vary by network and transaction volume</li> </ul> </li> <li>• Acquirers and issuers typically have a direct relationship with payment card brands and are primarily responsible for enforcement</li> <li>• Merchants and service providers are contractually obligated to comply with the standards</li> <li>• PCI SSC is not involved in compliance actions</li> </ul>	<p><b>What results have been achieved?</b></p> <ul style="list-style-type: none"> <li>• Has become the de facto minimum standard of compliance for storing, processing, and transmitting cardholder data</li> <li>• Improved data security practices have likely contributed to decreasing fraud losses from credit cards</li> <li>• Consumers can trust merchant businesses with credit card data</li> </ul>

<sup>1</sup> Pew Research Center, Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information, <https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/>.

<sup>2</sup> While there are many ways to parse and define health data, for the purposes of this paper, we contemplate a broad view inclusive of many types of digital information that relates to the physical or mental health of an individual or to the provision of health and wellness services to an individual that can be identified and attributed to that individual. However, we note particular concern for data that is currently subject to protections under HIPAA that loses that status once authorized by a patient/consumer to be released to a third party, such as an app vendor.

Examples of health data that might be considered in developing recommendations for a more robust privacy framework include (potentially among others):

- Patient information related to medical diagnosis and treatment, including health records, medical notes, lab test results, prescriptions, referrals and medical bills, among other elements, such as might typically be generated and recorded by entities within the healthcare system.
- Health-related data created, recorded or gathered by or from patients (or caregivers) to help address a health concern or interest, which may include, for example, biometric data, symptoms, remote monitoring using home health equipment, data from wellness applications or wearable devices, genomic analyses and health histories.
- Data relating to a specific health concern that is housed in a private registry and/or included in a health survey.
- Consumer online activity and behavioral data that could potentially be correlated to clinical conditions, such as consumer Internet search histories (such as those relating to health or medical-related topics); social media posts, “likes” and comments; participation in mobile text programs related to physical or behavioral health; and retail behavior and purchasing trends.
- Some stakeholders and analyses have also suggested that health-related data could include so-called online “proxy” data or information that may be mined to inform a picture of health status, such as residential data including ZIP code and housing status, geolocation data, socioeconomic factors, and information on the social determinants of health and data from the Internet of Things (such as smart home devices).

<sup>3</sup> <https://www.healthaffairs.org/doi/10.1377/hblog20190604.428654/full/>. Excerpt: “The proposed interoperability rules and the ONC Health IT Certification Program further federal efforts to ensure that electronic health information is available and can be securely and safely shared to improve the health and care of the American public. **We believe it is of utmost importance to implement these proposed interoperability rules as quickly as possible to propel the healthcare industry forward by finally enabling the meaningful flow of data.** In and of themselves, these rules do not, however, fully address patient and consumer privacy protections. **In parallel, we recommend that CMS and ONC, together with other relevant agencies and departments (such as the Department Health and Human Services (HHS) Office of Civil Rights and the Federal Trade Commission) and private-sector colleagues, develop a companion consumer privacy framework.**”

Consumers should clearly understand how their data is being used by third-party APIs and how to exercise their consent options. **A process should be put in place to ensure appropriate privacy protections are in place for consumers as the API market develops.”**

<sup>4</sup> 45 C.F.R. § 164.500(a).

<sup>5</sup> If a company offers an app or wearable on behalf of a covered entity, the company is a “business associate” under HIPAA and the data collected by the app or wearable is subject to HIPAA protections. See the box titled “Business Associate Agreements” on the following page.

<sup>6</sup> For more information on the limits of HIPAA in this context, see eHI’s and Manatt’s issue brief on the subject, [Risky Business? Sharing Data with Entities Not Covered by HIPAA](https://www.ehidc.org/resources/risky-business-sharing-data-entities-not-covered-hipaa) (also available at <https://www.ehidc.org/resources/risky-business-sharing-data-entities-not-covered-hipaa>).

<sup>7</sup> 45 C.F.R. Part 164, Subpart C.

<sup>8</sup> 42 C.F.R. §§ 2.11, 2.12.

<sup>9</sup> 20 U.S.C. § 1232g.

<sup>10</sup> Cal. Civ. Code § 56.06.

<sup>11</sup> <https://www.ftc.gov/news-events/press-releases/2016/08/ftc-approves-final-order-practice-fusion-privacy-case>.

<sup>12</sup> Cal. Civ. Code § 1798.140.

<sup>13</sup> Me. Stat. tit. 35-A, § 9301; Nev. Rev. Stat. § 604A.300 et al.

<sup>14</sup> Pub. L. 114–255.

<sup>15</sup> 85 FR 25642.

<sup>16</sup> 85 FR 25510. Medicaid, the Children’s Health Insurance Program (CHIP), Medicare Advantage (MA) plans and qualified health plans participating on federal insurance exchanges will need to make claims and encounter information as well as a subset of their clinical information through third-party APIs of their choice.

<sup>17</sup> <https://www.cms.gov/Regulations-and-Guidance/Guidance/Interoperability/index>; <https://www.healthit.gov/curesrule/resources/enforcement-discretion>.

<sup>18</sup> <https://www.hhs.gov/about/news/2020/04/21/statements-from-onc-cms-on-interoperability-flexibilities-amid-covid19-public-health-emergency.html>.

<sup>19</sup> “IoT in Healthcare Market Worth \$534.3 Billion By 2025,” Grand View Research, March 2019.

<sup>20</sup> <https://healthitanalytics.com/news/big-data-to-see-explosive-growth-challenging-healthcare-organizations>; December 2018.

<sup>21</sup> National Telecommunications and Information Administration (NTIA), U.S. Department of Commerce and U.S. Census Bureau, “Current Population Survey (CPS) Computer and Internet Use Supplement, 2017.”

<sup>22</sup> <https://www.hhs.gov/about/news/2020/03/09/hhs-finalizes-historic-rules-to-provide-patients-more-control-of-their-health-data.html>.

<sup>23</sup> “Mobile Application Market by Marketplace (Apple iOS Store, Google Play Store, and Other Marketplaces) and App Category: Global Opportunity Analysis and Industry Forecast, 2019-2026,” November 2019, Allied Market Research.

<sup>24</sup> The National Committee on Vital and Health Statistics recently published a report on core data privacy issues in healthcare and recommendations on a policy framework for more comprehensive data privacy: “[Health Information Privacy Beyond HIPAA: A Framework for Use and Protection; A Report for Policy Makers, June 18, 2019](https://ncvhs.hhs.gov/wp-content/uploads/2019/07/Report-Framework-for-Health-Information-Privacy.pdf)” (also available at <https://ncvhs.hhs.gov/wp-content/uploads/2019/07/Report-Framework-for-Health-Information-Privacy.pdf>).

<sup>25</sup> The CARIN Alliance is a group of more than 85 multi-sector stakeholders that includes health plans, providers, hospitals, third-party applications, consumer platform companies, EHR vendors, health plan technology systems, patient and caregiver advocates, and others. CARIN’s board of directors includes representatives from Alliance for Nursing Informatics, Apple, the Argonaut Project/HL7, b.well Connected Health, Cambia Health Solutions, Caregiver Action Network, CareJourney, Cedars-Sinai Health System, Ciiitizen, Electronic Health Records Alliance, Marshfield Clinical Health System, Microsoft, National Partnership for Women and Families, and New York Presbyterian.

<sup>26</sup> Xcertia’s board of directors includes representatives from Accenture, American Heart Association, AMA, DHX Group, HIMSS, IBM Watson Health, IQVIA, Mayo Clinic, Partners Connected Health, Alliance for Nursing Informatics, American Telemedicine Association and The App Association.

<sup>27</sup> CTA’s executive board includes representatives from Sony Electronics, IBM Global Technology Services, New Age Electronics (a division of SYNEX Corporation), Boingo, Vox International Corp., Starpower, Lutron, SVS, Sprint, Facebook, HP Inc., TargetPath, Robert Bosch LLC, Elemental and Soft Robotics. A list of CTA’s full membership can be accessed at <https://members.cta.tech/cta-member-directory>.

<sup>28</sup> Anil K. Gupta and Lawrence J. Lad, “Industry Self-Regulation: An Economic, Organizational, and Political Analysis,” *The Academy of Management Review* 8, no. 3 (1983): 417.

<sup>29</sup> Federal Trade Commission, “Self-Regulation in the Alcohol Industry,” June 2008, <http://www.ftc.gov/os/2008/06/080626alcoholreport.pdf>.

<sup>30</sup> The Better Business Bureau’s nonprofit organization, BBB National Programs, is the home of independent self-regulatory and dispute resolution programs that include the National Advertising Division, National Advertising Review Board, BBB EU Privacy Shield, BBB AUTO LINE, Children’s Advertising Review Unit, Children’s Food and Beverage Advertising Initiative, Children’s Confection Advertising Initiative, Direct Selling Self-Regulatory Council, Electronic Retailing Self-Regulation Program, Digital Advertising Accountability Program and the Coalition for Better Advertising Dispute Resolution Program.

<sup>31</sup> The FTC has periodically recommended Congress enact legislation to protect consumer privacy as related to online data gathering, and across 2007–2009, the agency promulgated recommendations for an industry-led, self-regulatory approach, stating that such a model would provide a necessary flexibility to address evolving business models in a developing market. Federal Trade Commission Staff Report: Self-Regulatory Principles For Online Behavioral Advertising: Tracking, Targeting, and Technology (February 2009).

<sup>32</sup> Card brands that operate a closed loop system, like American Express, may not use an issuing or acquiring bank and have a different enforcement system.

manatt

Albany

Boston

Chicago

Los Angeles

New York

Orange County

Palo Alto

Sacramento

San Francisco

Washington, D.C.