## EXECUTIVE SUMMARY

Health care data privacy is at the heart of consumer trust in health care. Consumers want to trust that the health care system will not only keep them healthy, but also protect their most sensitive information.

The foundation of that trust must be continually assessed and strengthened as technology is leveraged in new and innovative ways to deliver care, and vast amounts of data are being generated, aggregated and used across the health care ecosystem. This includes data generated in clinical settings like a hospital or physician office, but also data captured by consumers through apps and wearables and data used in and generated from artificial intelligence (AI) and other machine learning techniques.

The privacy and security of this information is governed by a patchwork of federal and state laws. While the federal Health Insurance Portability and Accountability Act (HIPAA) protects health data maintained by payers, providers, and health care clearinghouses - health and other sensitive data is increasingly generated by or shared with new digital health tools or technologies that fall outside of HIPAA's protections. Beyond HIPAA, there are no comprehensive data privacy rules in place at the federal level, however several states have enacted additional data privacy protections and both Congress and the Administration have recently taken steps to move towards a more active approach to addressing data privacy, including health data privacy.

In December 2022, a wide range of organizations representing clinicians, hospitals, payers, technology companies, and consumer advocates came together to jointly host a event on Maintaining Consumer Trust in Health Care Through Data Privacy and Patient Access.[1]

Roundtable participants discussed the overall importance of maintaining consumers' trust and right to access, and control access to, their health care data; opportunities and challenges created by existing regulatory frameworks for both HIPAA-covered and non-HIPAA covered health data; perceived gaps in data privacy and Congressional and Administration actions to address those gaps; and recommendations for moving forward.

This White Paper summarizes many of the key conversations and perspectives raised during the event, as well as key considerations for moving forward. The White Paper: (1) highlights limitations or gaps in HIPAA's protection of health data and what current laws or protections exist at the state or federal level for health information that is not protected by HIPAA; (2) details recent actions taken by Congress and the Administration to advance consumer and patient access to their health information, while also maintaining adequate protections for health information; and (3) discusses the data privacy and consumer trust implications associated with new and emerging technologies that are becoming more commonplace in health settings.

[1] See Appendix for the agenda for the Health IT Leadership Roundtable – Maintaining Consumer Trust in Health Care Through Data Privacy and Patient Access. This is the fifth Health IT Leadership Roundtable convened by the Host Committee. For more information on previous Roundtable events and topics, see https://sironastrategies.com/tag/health-it-leadership-rountable

to be used as an educational manual for medical professionals that focused on dispelling myths around HIPAA and helping physicians understand their obligations to provide health care consumers with access to their health information, including through a third party or app.[17]

Additionally, in January 2022 the College of Healthcare Information Management Executives (CHIME) and the Workgroup for Electronic Data Exchange (WEDI) developed the "THINK BEFORE YOU CLICK" resource that includes a five-step checklist to assist consumers who are looking to share their health information with third-party apps.[18]

Similarly, OCR released guidance in June of 2022 reminding consumers that HIPAA rules generally do not protect the privacy and security of individual health information when it is accessed through, stored, or shared via a personal cell phone, tablet, app, or other technology.[19]

HHS Office of the National Coordinator for Health IT, HHS, and OCR have also approved and/or published several resources to assist providers in understanding and better integrating HIPAA into their practice, including a booklet on HIPAA basics for providers.[20,21] Additionally, in December 2022, HHS OCR issued a bulletin highlighting the obligations of HIPAA on regulated entities when using online tracking technologies, such

consumer data; and the Family Educational Rights and Privacy Act (FERPA) dictates who can request

targeted advertising. The bill also included enforcement mechanisms, and would create a division within the FTC charged with enforcing data privacy.[33]

As it is written, ADPPA could have significant implications for the sizable amount of health data that is generated or shared outside of HIPAA. For instance, ADPPA includes increased protections for individuals with regard to their "sensitive covered data," which includes health information. ADPPA notably attempts to reduce duplication by exempting information that is already regulated under certain federal laws, such as HIPAA, however some health care stakeholders have raised questions as to whether these exemptions are sufficient.

Thus, if enacted, although consumers and covered entities would still need to navigate gaps or differences between the two laws' privacy protections, ADPPA attempts to establish an inherent baseline set of protections for health information outside of HIPAA.

In addition to ADPPA, members of Congress have introduced several other pieces of legislation aimed at strengthening privacy and security protections for data, including health data. For instance, in February 2022 Sen. Tammy Baldwin (D-WI) and Sen. Bill Cassidy (R-LA) introduced the Health Data Use and Privacy Commission Act, which would establish a Commission to review gaps in how current laws protect health data privacy; in August 2022, Sen. Amy Klobuchar (D-MN) introduced the Stop Commercial Use of Health Data Act, which would prohibit covered entities from using personally-identifiable health data for commercial advertising purposes; and in November 2021 Senate Commerce Committee Chair Marie Cantwell (D-WA) introduced the Consumer Online Privacy Rights Act, a broader data privacy bill, which would place requirements on entities that process or transfer a consumer's data.[34,35,36]

Several lawmakers have also introduced legislation to improve the protection of collected by health tracking devices and apps (and thus existing beyond the walls of HIPAA), as well as legislation to protect reproductive health data – largely as a response to the Supreme Court decision in the

.[37]

For instance, in June 2022, Rep. Sara Jacobs (D-CA) introduced the My Body, My Data Act, which would create a national standard to protect personal reproductive health data.[38]

---

[33] Congressional Research Service, "Overview of the American Data Privacy and Protection Act, H.R. 8152." Available here: https://crsreports.congress.gov/product/pdf/LSB/LSB10776#:~:text=Private%20right%20of%20action.,-The%20bill%20would&text=Injured%20individuals%2C%20or%20classes%20of,attorney%20general%20before%20bringing%20suit

[34] Health Data Use and Privacy Commission Act (S.3620). Available here: https://www.congress.gov/bill/117th-congress/senate-bill/3620?s=1&r=2

[35] Stop Commercial Use of Health Data Act (S. 4738). Available here: https://www.congress.gov/bill/117th-congress/senate-bill/4738/text?r=10&s=1

[36] Consumer Online Privacy Rights Act (S. 3195). Available here: https://www.congress.gov/bill/117th-congress/senate-bill/3195?q=%7B%22search%22%3A%5B%22cantwell%22%2C%22cantwel

## STATE APPROACHES TO DATA PRIVACY

Given the complexity of the current data economy and the lack of federal protections, several states have stepped in to enact state-level laws regulating data privacy. The California Consumer Privacy Act (CCPA), which came into effect on January 1, 2020, made California the first state with a comprehensive consumer privacy law and gave Californians new rights concerning their personal information.[39] The CCPA and the California Privacy Rights Act (CPRA), a ballot measure approved by California voters in November 2020, catalyzed an emergence of proposed state privacy laws across several other states. [13]

State-level momentum for comprehensive privacy laws has rapidly increased to fill the void left by federal lawmakers. In 2022, 60 comprehensive consumer privacy bills were considered across 29 states, resulting in an increase of 106 percent in bills considered between 2022 and 2021, when only 29 bills were considered.[40] In addition, five states (Georgia, Indiana, Maine, Michigan, and Vermont) considered comprehensive consumer privacy bills for the first time and two states (Connecticut and Utah) passed new consumer privacy laws. Both the Connecticut and Utah laws, effective July 1, 2023 and December 31, 2023 respectively, considered "sensitive data" to include data or information regarding an individual's mental or physical health or diagnosis.[41,42] Additionally, both laws, similar to the CCPA as amended by the California Privacy Rights Act (CPRA), contain exemptions for covered entities, business associates and protected health information subject to HIPAA.

## INDUSTRY & STAKEHOLDER ACTION

As the Administration, Congress, and states contemplate and take steps to modernize data privacy laws and rules, several health care stakeholder organizations have worked to identify key health data privacy principles and recommendations for their consideration.

For instance, in March 2022, the Executives for Health Innovation (EHI) released a report with guidance for protecting non-HIPAA-covered health data held by health tech companies.[43] In the report, EHI advocated for the adoption of industry-wide self-regulated standards for entities to follow. This report builds on previous work done by EHI and the Center for Democracy & Technology (CDT) when the organizations released a proposed Consumer Privacy Framework for Health Data in February 2021.[44] The Framework outlined gaps in legal protections and discussed how non-HIPAA-covered health data should

---

[39] Cali61 TJETQ0.000P /73Q0.0a ni -

## KEY TAKEAWAYS

Speakers and panelists participating in the Health IT Leadership Roundtable event on agreed that recent actions taken by the federal and state governments emphasize and advance the need to increase consumer and covered entity understanding of current health data protections, including HIPAA's limitations and how to best protect data shared or generated outside of HIPAA.

Moreover, as additional data privacy policies and legislation are considered, it is important to ensure that

## CONSUMER-CENTRIC

The onus to understand and ensure privacy policies are being properly followed currently falls on the consumer. This must change. Privacy policies are extremely long, difficult to understand, and not consumer friendly. Instead, there needs to be baseline rules that place limits on how health data is collected, shared, sold, and used. Strong rules will allow the consumer to know their health data will not be used in ways or for purposes that they did not know about, anticipate, and/or want.

## TRUST

One of the central tenets of health care is maintaining a culture of trust in the physician-patient relationship. It is crucial to provide good quality health care. Patient trust in physicians, a multi-dimensional perception influenced by patient, physician, and situational factors, can either enable, or hinder the accuracy and quality of the information a patient shares with their provider. Numerous reports and surveys have been published that emphasize the need for security and privacy assurances to improve consumer experience. These resources have also shown that transparency is a crucial element of building and maintaining patient trust.

## REGULATION

Regulation of information in the U.S. takes a sectoral approach. The federal government should have clear responsibilities for enforcing health data privacy protections both within and outside of HIPAA and ensuring that consumers have assurance that their rights are being upheld. Regulations governing the sharing and protection of patient health information must be harmonized to meaningfully improve patients' access to their health data and advance interoperability while safeguarding patient privacy and security. Any new authority should align fully with HIPAA and not duplicate or create additional burden and complexities for covered entities and consumers.

APPENDIX