MAINTAINING CONSUMER TRUST IN HEALTH CARE THROUGH DATA PRIVACY & PATIENT ACCESS

HEALTH IT LEADERSHIP ROUNDTABLE

FEBRUARY 2023

TABLE OF CONTENTS

EXECUTIVE SUMMARY.....3

INTRODUCTION.....4

HIPAA AND EFFORTS TO PROTECT HEALTH DATA PRIVACY.....4

PROTECTING NON-HIPAA COVERED HEALTH DATA.....7

KEY TAKEAWAYS.....12

APPENDIX.....14

HEALTH IT LEADERSHIP ROUNDTABLE HOST COMMITTEE

American Academy of Family Physicians | American College of Physicians | American Health Information Management Association | American Heart Association | American Hospital Association | American Medical Group Association| Blue Cross Blue Shield Association | Center for Democracy and Technology | College of Healthcare Information Management Executives | Consumer Technology Association | Federation of American Hospitals | Medical Group Management Association | National Partnership for Women & Families | Premier Healthcare Alliance

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 *Health IT Leadership Roundtable* 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 *Roundtable* 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

INTRODUCTION

There is currently no singular law that governs the privacy of all types of consumer data in the U.S. Instead, the U.S. has a sectoral and ever-evolving network of laws that either govern specific types of data, focus on specific situations regarding privacy, or address privacy for specific populations. Efforts at the federal level to pass comprehensive data privacy legislation have been ongoing for nearly two decades, with major divisions in Congress stymying several significant attempts to reform data privacy laws in recent years.

In the absence of any major federal data privacy policy, state legislatures have begun to take the lead on enacting consumer data privacy laws. At least five states – California, Colorado, Connecticut, Utah, and Virginia – have recently enacted laws, guaranteeing data privacy rights to consumers in their states and over a dozen other states are considering passing similar laws.[2]

These bills come at a critical time with the continuing digitization of health care and the growing popularity and use of health technologies and apps that collect, store, and share personal health data. These ubiquitous devices and services have expanded the volume and variety of health data collected, stored, and analyzed by a wide range of entities.

When it comes to health data, consumers have limited protections beyond the Health Insurance Portability and Accountability Act (HIPAA). HIPAA's rules were designed to support and protect information flows within the health care system and allow for certain uses and disclosures of data by both covered entities and business associates. However, many third parties, such as health apps, often fall outside HIPAA's purview, positioning them in a regulatory gray area where transparency, security, and privacy obligations are not clearly defined. Most consumers remain unclear on which rule(s) govern and protect their data privacy and many have expressed concern over the lack of security and confidentiality of their personal health information.[3]

In an era of expanded data sharing, without clear guardrails around ethical use of health data and adequate consumer and provider education around existing protections, public trust in health data privacy suffers. As health information sharing extends beyond health systems to be more inclusive of a diverse set of third-party consumer apps, technologies, and other platforms, it is imperative that consumer trust remains a top priority. To build on the progress made in empowering consumers to play a more active role in their health care by accessing and contributing to their data, health care stakeholders must continue to promote both consumer and provider education. Additionally, federal and state governments must work to advance comprehensive privacy solutions that better protect health data, maintain consumer trust, and ensure clear guidelines for health care providers and other entities, without increasing burden.

HIPAA AND EFFORTS TO PROTECT HEALTH DATA PRIVACY

In 2020, HHS proposed the first major updates to the HIPAA Privacy Rule in almost 20 years, seeking to update the regulations to provide consumers with easier access to their health information, including through the use of personal health record apps, enhance information sharing for care coordination and

[2] International Association of Privacy Professionals (IAPP), "US State Privacy Legislation Tracker 2023." Available here: https://iapp.org/media/pdf/resource_center/State_Comp_Privacy_Law_Chart.pdf

[3] American Medical Association (AMA), "Patient survey shows unresolved tension over health data privacy." July 2022. Available here: https://www.ama-assn.org/press-center/press-releases/patient-survey-shows-unresolved-tension-over-health-data-privacy

case management, and reduce the administrative burden on HIPAA-covered entities, among other proposals.[4]

While HHS has not yet finalized this proposed rule, the Department has continued to take other actions to improve interoperability and exchange of health data and patient access to health information, which collectively serve to accelerate the exchange and use of electronic health information across entities.[5,6,7]

However, while HIPAA regulates the flow of information between HIPAA-covered entities, the law has limited ability to protect health data shared with non-HIPAA-covered entities and often does not cover information shared with third parties, including apps and other technologies.[8]

HIPAA AND THIRD-PARTY DATA SHARING

Under certain circumstances, such as when patients opt to share their data with a third party under the HIPAA Patient Right of Access, health care organizations and their vendors are not required to have a business associate agreement with a third-party app developer to transmit data to that app.[9] Moreover, when PHI is shared with a third-party app or a patient requests their health care provider or another entity share their health data with an app, the HHS Office for Civil Rights (OCR) has clarified that the covered entity is often not liable for any subsequent use or disclosure of the data as long as the app developer is not a business associate of the covered entity.[10]

> *"One thing is clear, digital health tools are here to stay. Their importance is only going to grow. We must realize that people are going to continue to rely on these devices and software tools. It is also important to remember that HIPAA was never intended to be a comprehensive privacy law for all health data."* – HITR Panelist

Beyond HIPAA, other laws protecting against deceptive or unfair acts or breaches of privacy may apply in certain circumstances, as described further below, including the Federal Trade Commission (FTC) Act,

---

[4] U.S. Department of Health and Human Services (HHS), "HHS Proposes Modifications to the HIPAA Privacy Rule to Empower Patients, Improve Coordinated Care, and Reduce Regulatory Burdens." December 2020. Available here: https://public3.pagefreezer.com/content/HHS.gov/31-12-2020T08:51/https:/www.hhs.gov/about/news/2020/12/10/hhs-proposes-modifications-hipaa-privacy-rule-empower-patients-improve-coordinated-care-reduce-regulatory-burdens.html

[5] Centers for Medicare and Medicaid Services (CMS), "Advancing Interoperability and Improving Prior Authorization Processes Proposed Rule CMS-0057-P: Fact Sheet." December 2022. Available here: https://www.cms.gov/newsroom/fact-sheets/advancing-interoperability-and-improving-prior-authorization-processes-proposed-rule-cms-0057-p-fact

[6] CMS, "Administrative Simplification: Adoption of Standards for Health Care Attachments Transactions and Electronic Signatures, and Modification to Referral Certification and Authorization Transaction Standard." December 2022. Available here: https://www.cms.gov/newsroom/fact-sheets/administrative-simplification-adoption-standards-health-care-attachments-transactions-and-electronic

[7] HHS Office of the National Coordinator for Health IT (ONC), "The ONC Cures Act Final Rule." Available here: https://www.healthit.gov/sites/default/files/page2/2020-03/TheONCCuresActFinalRule.pdf

[8] Under HIPAA, protected health information is considered to be individually identifiable health relating to the past, present, or future health status of an individual that is created, collected, transmitted, or maintained by a HIPAA-covered entity in relation to the provision of health care, payment for health care services, or use in health care operations. HIPAA requires providers, payers, and other entities managing patients' health information to restrict access, disclosure, and use of health information, except for certain authorized purposes, such a treatment, payment and operations, or unless expressly authorized by a patient.

[9] HHS, "The access, right, health apps, & APIs." Available here: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/access-right-health-apps-apis/index.html#:~:text=HIPAA%20does%20not,another%20business%20associate

[10] Id.

the FTC's Health Breach Notification Rule, or state laws such as the California Privacy Rights Act.[11,12,13] The gaps in standards between HIPAA and the limited protections offered by other laws can lead to confusion and the web of requirements creates additional complexity and burden for both patients as they seek to understand their rights, and providers, as they seek to maintain compliance and trust with their patients.[14]

Consumers may not understand when their data is protected by HIPAA, a different applicable law, or not at all.[15] Moreover, the onus is often placed on the consumer to interpret a device's or app's privacy policy, which is often lengthy, can change over time with little notice, and may allow downstream disclosure and use of sensitive health data. Additionally, relying on the patient's physician to determine whether a device or app has appropriate security and privacy places a significant burden on physician practices, who are likely unequipped to make this determination or provide adequate patient education on app security.

> *"When consumers go in to see a doctor, they have this feeling that this information is going to be protected. When you're talking about the same or similar information that is being collected and generated outside of HIPAA, you have consumers not really understanding that there are different or lesser protections that might apply."* – HITR Panelist

Additionally, providers and other covered entities are increasingly caught between HIPAA's protective standards, a constellation of other federal and state privacy laws, and incentives for greater information sharing created through new regulatory policies (e.g., information blocking).[16]

INDUSTRY & GOVERNMENT ACTION

Panelists throughout the Health IT Leadership Roundtable event lamented the confusing and challenging current approach to health data privacy, with one panelist arguing, "*In the current environment, it's on each and every individual to take the time to determine what they're comfortable with. If you were actually to do that, that's an immense amount of time. It's an unworkable system. We really need to readjust the levers here and put more responsibility on the entities that are collecting and using that data to say what are acceptable data practices and what are unacceptable practices."* Adding on to that, another panelist noted *"A 2008 study had indicated that for a person to read every privacy policy they encounter in a year, it would take 76 days. That is unrealistic and not consumer centric and friendly."*

Industry, as well as the federal government, have taken recent actions to address patient privacy concerns regarding health data sharing, and to enhance consumer understanding of the current limitations in protection offered by HIPAA as it relates to electronic health information.

Many covered entities seeking to protect consumers and maintain their trust have developed educational and other resources. For instance, in 2020, AMA published a Patient Records Electronic Access Playbook

---

[11] Federal Trade Commission (FTC), "Federal Trade Commission Act." Available here: https://www.ftc.gov/legal-library/browse/statutes/federal-trade-commission-act

[12] FTC, "Health Breach Notification Rule." Available here: https://www.ftc.gov/legal-library/browse/rules/health-breach-notification-rule

[13] California Privacy Rights Act of 2020. Available here: https://iapp.org/media/pdf/resource_center/ca_privacy_rights_act_2020_ballot_initiative.pdf

[14] Vox, "HIPAA, the health privacy law that's more limited than you think, explained." July 2021. Available here: https://www.vox.com/recode/22363011/hipaa-not-hippa-explained-health-privacy

[15] American Health Information Management Association (AHIMA), "Making HIPAA Work for Consumers: Teaching How and Why to Access Health Records." Available here: https://bok.ahima.org/doc?oid=302049#.Y9gYGnbMIuV

[16] 45 CFR § 171.103 Information blocking.

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 as Google Analytics or Facebook's Meta Pixel, that collect and analyze information about how internet users are interacting with a regulated entity's website or mobile app.[22] Finally, In December 2022, the FTC released an updated Mobile Health App Interactive Tool to help developers determine what federal laws and regulations apply to apps that collect and process health data.[23]

PROTECTING NON-HIPAA COVERED HEALTH DATA

As noted in the previous section, the United States does not have a comprehensive law governing data collection, protection, and privacy of individually identifiable data. Instead, there is a system of federal and state laws that govern particular sectors and types of personal information.[24] For example, the FTC has authority to limit companies from engaging in unfair and deceptive practices and protects against health data breaches.[25]

Separately, the Fair Credit Reporting Act (FCRA) protects information found in credit reports; the Children's Online Privacy Protection Act (COPPA) protects children's (under the age of 13) online privacy; the Gramm-Leach-Bliley Act (CLBA) requires consumer financial products to explain how they share

---

[17] American Medical Association (AMA), "Patient Records Electronic Access Playbook." 2020. Available here: https://www.ama-assn.org/system/files/2020-02/patient-records-playbook.pdf

[18] College of Health Information Management Executives (CHIME), "THINK BEFORE YOU CLICK." January 2022. Available here: https://chimecentral.org/wp-content/uploads/2022/05/ThinkBeforeYourClick_Jan2022REVISEDMay162022_CHIME.pdf

[19] HHS, "Protecting the Privacy and Security of Your Health Information When Using Your Personal Cell Phone or Tablet." Available here: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html

[20] ONC, "Health IT Privacy and Security Resources for Providers." Available here: https://www.healthit.gov/topic/privacy-security-and-hipaa/health-it-privacy-and-security-resources-providers

[21] CMS, "HIPAA Basics for Providers: Privacy, Security, & Breach Notification Rules." May 2021. Available here: https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/HIPAAPrivacyandSecurity.pdf

[22] OCR, "Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates." Available here: https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html

[23] FTC, "Mobile Health App Interactive Tool." Available here: https://www.ftc.gov/business-guidance/resources/mobile-health-apps-interactive-tool

[24] The New York Times – Wirecutter, "The State of Consumer Data Privacy Laws in the US (And Why It Matters)." September 2021. Available here: https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/

[25] Federal Trade Commission (FTC), "Health Privacy." Available here: https://www.ftc.gov/business-guidance/privacy-security/health-privacy

consumer data; and the Family Educational Rights and Privacy Act (FERPA) dictates who can request student education records.[26,27,28,29]

While each of these laws protects data shared for a certain purpose, the data collected by the vast majority of products and technologies consumers use most often, if not every day, remains largely unregulated. For example, geolocation data, which is continuously collected via smartphones through a myriad of sources (e.g., GPS, Wi-Fi, Bluetooth signals etc.) can be used by third-parties to advertise health-related products by virtue of where a person is located or where a person is visiting.

FEDERAL APPROACHES TO DATA PRIVACY

There is strong, widespread public support for establishing more comprehensive federal data privacy protections and a growing sentiment among policymakers that privacy laws and rules should be assessed to account for the evolution of emerging technologies and data management tools, including the treatment of sensitive data, such as health data.[30]

Recently, the FTC issued an Advance Notice of Proposed Rulemaking (ANPR) seeking comments on potential harms stemming from commercial surveillance and data security and whether new rules are needed to protect people's privacy and information, including sensitive data.[31] The ANPR also recognized that the FTC may have limited statutory authority to issue rules, given its limited jurisdiction over data privacy, so it is unclear how the FTC will proceed and how any new rulemaking would interact with existing rules, such as the HIPAA Privacy Rule.

Separately, Congress has long attempted to enact a comprehensive national standard that would modernize current laws and fill gaps in privacy protections, arguing that the current collection of laws leads to confusion and complexity. Fundamental policy disagreements, such as state preemption and whether consumers should have a private right of action have stymied most legislative efforts to-date.

The American Data Privacy and Protection Act (ADPPA) sought to find compromise solutions to these longstanding policy disagreements, and progressed further than any other recent data privacy bill.[32] ADPPA was introduced in June 2022 by bipartisan leaders of the House Energy & Commerce Committee (E&C), Reps. Frank Pallone (D-NJ) and Cathy McMorris Rodgers (R-WA), and the Ranking Member of the Senate Commerce Committee, Sen. Roger Wicker (R-MS).

E&C advanced ADPPA by a vote of 53-2 in July 2022 to the full House for consideration, however the bill ultimately failed to pass during the 117th Congress and is expected to be reintroduced in the 118th Congress. ADPPA would have created a comprehensive framework and standards for how companies handle personal data, including information that is reasonably identifiable. The bill establishes consumer data protections, including the right to access, correct, and delete personal data, and limitations on

---

[26] FTC, "Fair Credit Reporting Act." Available here: https://www.ftc.gov/legal-library/browse/statutes/fair-credit-reporting-act

[27] FTC, "Children's Online Privacy Protection Act." Available here: https://www.ftc.gov/legal-library/browse/statutes/childrens-online-privacy-protection-act

[28] FTC, "Gramm-Leach-Bliley Act." Available here: https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act

[29] U.S. Department of Education, "Family Educational Rights and Privacy Act (FERPA)." Available here: https://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

[30] Morning Consult, "Voters Overwhelmingly Back Major Provisions of Proposed Federal Data Privacy Law." June 2022. Available here: https://morningconsult.com/2022/06/15/support-for-federal-data-privacy-law/

[31] FTC, "Trade Regulation Rule on Commercial Surveillance and Data Security." August 2022. Available here: https://www.federalregister.gov/documents/2022/08/22/2022-17752/trade-regulation-rule-on-commercial-surveillance-and-data-security

[32] American Data Privacy and Protection Act (ADPPA) (H.R. 8152). Available here: https://www.congress.gov/bill/117th-congress/house-bill/8152?r=29

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

> "*The beauty of ADPPA is that it's not based on consent. You don't need everyone clicking on a box every time they go to a new website. Consumers get a baseline consumer protection standard, so they know when they use a product, that that business is complying to a standard*." – HITR Panelist

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 *Dobbs v. Jackson Women's Health Organization*.[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%22cantwell%22%5D%7D&s=6&r=13

[37] SCOTUS blog, "Dobbs v. Jackson Women's Health Organization." Available here: https://www.scotusblog.com/case-files/cases/dobbs-v-jackson-womens-health-organization/

[38] My Body, My Data Act of 2022 (H.R. 8111). Available here: https://www.congress.gov/bill/117th-congress/house-bill/8111?q=%7B%22search%22%3A%5B%22my+body+my+data%22%2C%22my%22%2C%22body%22%2C%22data%22%5D%7D&s=1&r=2

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]

> *"One challenge for lawmakers is to try to address these gaps in the law and keep up with new technologies while working in a federal system. That's part of the reason why state privacy law has evolved the way it has."* – HITR Panelist

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] California Consumer Privacy Act of 2018. Available here: https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

[40] International Association of Privacy Professional (IAPP), "Privacy Matters in the US States." Available here: https://iapp.org/media/pdf/resource_center/infographic_privacy_matters_in_the_us_states.pdf

[41] State of Connecticut, "Public Act No. 22-15." Available here: https://www.cga.ct.gov/2022/ACT/PA/PDF/2022PA-00015-R00SB-00006-PA.PDF

[42] State of Utah, "Consumer Privacy Act." Available here: https://le.utah.gov/~2022/bills/static/SB0227.html

[43] Executives for Health Innovation (EHI), "The Case for Accountability: Protecting Health Data Outside the Healthcare System." Available here: https://www.ehidc.org/sites/default/files/Report_The%20Case%20for%20Accountability_2022.pdf?utm_source=Website&utm_medium=Report&utm_campaign=PrivacyFramework_2022

[44] Center for Democracy & Technology (CDT), "CDT & eHI's Proposed Consumer Privacy Framework for Health Data." February 2021. Available here: https://cdt.org/insights/cdt-ehis-proposed-consumer-privacy-framework-for-health-data/

be used, accessed, and disclosed. In their more recent report, EHI makes the case for a stronger system of accountability to govern the use of health data held and used by health tech companies.

Similarly, in September 2019, the Consumer Technology Association (CTA) released a set of industry-developed voluntary privacy guidelines for companies that handle consumer health and wellness data collected from devices, apps, websites, and other digital tools.[45]

In May 2020 the American Medical Association (AMA) published a set of privacy principles that aimed to provide consumers with meaningful control over and a clear understanding of how their health care data is being used and with whom it is being shared.[46] The principles seek to provide individuals with rights and protections from discrimination and shifted the responsibility for privacy from individuals to data holders. As AMA states in these principles, "third parties who access an individual's data should act as responsible stewards of that information, just as physicians promise to maintain patient confidentiality".

Additionally, in July 2020 the CARIN Alliance released a set of principles for how health care organizations should share data with consumer apps. The CARIN Trust Framework and Code of Conduct sought to advance the ability for consumers and their authorized caregivers to easily obtain, use, and share digital health information to achieve health goals.[47] The framework is primarily focused on solving use cases around how a consumer electronically requests access to their data using APIs, indicates where it should be sent, and is informed how their data will be used, and how a covered entity electronically sends that data to the consumer.

[45] Consumer Technology Association (CTA), "Guiding Principles for the Privacy of Personal Health Data." September 2019. Available here: https://cdn.cta.tech/cta/media/media/membership/pdfs/final-cta-guiding-principles-for-the-privacy-of-personal-health-and-wellness-information.pdf

[46] American Medical Association (AMA), "AMA Privacy Principles." May 2020. Available here: https://www.ama-assn.org/system/files/2020-05/privacy-principles.pdf

[47] CARIN Alliance, "The CARIN Trust Framework and Code of Conduct." May 2020. Available here: https://www.carinalliance.com/wp-content/uploads/2020/07/2020_CARIN_Code_of_Conduct_May-2020.pdf

KEY TAKEAWAYS

Speakers and panelists participating in the Health IT Leadership Roundtable event on *Maintaining Consumer Trust in Health Care Through Data Privacy and Patient Access* 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 the responsibility for data stewardship is not fully burdened by the consumer nor should new policies place unnecessary burden on HIPAA covered entities. Steps taken by state and federal governments should aim to balance the promotion of patient access to their health information with adequate, appropriate, and enforceable privacy protections vital to maintaining consumer privacy and trust.

Additional key takeaways from the Health IT Leadership event include the following:

OVERALL

Data privacy needs to be a multisector discussion. Government agencies with jurisdiction in this space should work with and across other agencies, as well as with industry stakeholders to generate solutions that address consumer access to and control of their health data. A primary tenant of any privacy law should be to ensure individuals' health information is properly protected while allowing for the flow of health information needed to promote high quality health care and protect the public's health and wellbeing.

EDUCATION

Data privacy is complex. The average consumer and/or patient is not and should not be expected to become a HIPAA expert and therefore, is likely unaware of where HIPAA protections for health data start and stop. Commercial app companies generally are not HIPAA-covered entities. Therefore, when information flows from a covered entity's information system to an app, it may no longer be protected by HIPAA. Third-party apps and digital health tools are here to stay, and consumers and providers need to be informed on how, with whom, and in what ways their data is being shared or stored. Innovative tactics and strategies need to be deployed to increase consumer understanding and awareness. Additionally, there needs to be resources in place for providers to educate themselves on the various privacy laws at play that govern health data sharing.

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

Health care data privacy is at the heart of consumer trust in health care. Technology is increasingly being used in new and innovative ways to deliver care, and increasing amounts of data are being generated, aggregated and used across the health care system.

Join leaders across the health care system in a virtual discussion of the importance of maintaining trust in health care through policies that protect data privacy and ensure secure patient access to their health information.

AGENDA

Opening Remarks
- Gary Anderson, Senior Vice President, Chief Information Officer, GuideWell and Florida Blue

Administration Keynote - Maintaining Health Data Privacy & Patient Access to their Health Information
- Melanie Fontes Rainer, Director, HHS Office for Civil Rights

Panel #1: Maintaining Health Data Privacy & Patient Access to their Health Information
- *Moderator:* Brooke McSwain, National Policy Research Analyst, American Heart Association
- Ashok Chennuru, Chief Data and Analytics Officer, Elevance Health
- Graham Dufault, Senior Director for Public Policy, ACT | The App Association
- Mari Savickis, Vice President, Public Policy, CHIME

State Perspectives - Navigating State Approaches to Protecting Data Privacy
- Müge Fazlioglu, Principal Researcher - Privacy Law and Policy, International Association of Privacy Professionals (IAPP)

Congressional Remarks
- Rep. Sara Jacobs (D-CA)
- Sen. Amy Klobuchar (D-MN), Chair of the Senate Judiciary Committee, Subcommittee on Competition Policy, Antitrust, and Consumer Rights
- Sen. Roger Wicker (R-MS), Ranking Member of the Senate Committee on Commerce, Science, and Transportation

Panel #2: Protecting Non-HIPAA Covered Health Data
- *Moderator:* Lauren Choi, Managing Director, Health Data and Technology Policy, Blue Cross Blue Shield Association
- David Brody, Managing Attorney, Digital Justice Initiative, Lawyers' Committee for Civil Rights Under Law
- Andy Crawford, Senior Counsel, Data and Privacy Project, Center for Democracy and Technology
- Nadia Daneshvar, Associate, Health IT Policy, American College of Physicians
- Cora Han, Chief Health Data Officer, UC Health

Closing Remarks
- Kristen McGovern, Partner, Sirona Strategies