American College of Physicians
Leading Internal Medicine, Improving Lives

July 28, 2022

The Honorable Nancy Pelosi
Speaker
U.S. House of Representatives
Washington, DC 20515

The Honorable Kevin McCarthy
Minority Leader
U.S. House of Representatives
Washington, DC 20515

Dear Speaker Pelosi and Minority Leader McCarthy:

On behalf of the American College of Physicians (ACP), I am writing to express our views on the growing crisis surrounding health information privacy and applaud recent efforts by the Energy and Commerce Committee to improve data privacy protections through H.R. 8152, the American Data Privacy and Protection Act (ADPPA), which was recently approved by that Committee. We appreciate the opportunity to offer the physician perspective on this important bipartisan and bicameral legislation, the first of its kind, to establish a comprehensive federal consumer data privacy framework, which has been an ACP priority for many years. Our comments will focus on key provisions of this legislation in relation to our established principles on health information privacy, as outlined below. We also emphasize the need to ensure such privacy protections adequately safeguard medical research on human subjects and are extended to reproductive health information in the wake of the Supreme Court decision to overturn *Roe v. Wade.*

The ACP is the largest medical specialty organization and the second-largest physician membership society in the United States. The ACP members include 160,000 internal medicine physicians (internists), related subspecialists, and medical students. Internal medicine physicians are specialists who apply scientific knowledge, clinical expertise, and compassion to the preventive, diagnostic, and therapeutic care of adults across the spectrum from health to complex illness. Internal medicine specialists treat many of the patients at greatest risk from COVID-19, including the elderly and patients with pre-existing conditions such as diabetes, heart disease, and asthma.

In its 2021 position paper, as published in the *Annals of Internal Medicine*, ACP built its health information privacy policy for the evolving digital health landscape on six key principles:

- Protecting the privacy and security of personal health information collected both within and outside the health care system—while providing individual rights to that information—is essential for fostering trust in the evolving digital health care system, maintaining ethical standards and respect for persons, and promoting the safe delivery of health care.

- Increasing transparency and public understanding and improving models of consent about the collection, exchange, and use of personal health information within existing Health Insurance Portability and Accountability Act (HIPAA) rules as well as for entities collecting, exchanging, and using personal health information outside the health care system.

- Supporting the confidentiality of personal health information as a fundamental aspect of medical care, and physicians and other clinicians have an obligation to adhere to appropriate privacy and security protocols to protect individual privacy.

- Believing that health IT and other digital technologies, including personalized digital health products, should incorporate privacy and security principles within their design as well as consistent data standards that support privacy and security policies and promote safety.

- Supporting oversight and enforcement to ensure that all entities not currently subject to HIPAA rules and regulations and that interact with personal health information are held accountable for maintaining confidentiality, privacy, and security of that information.

- Believing that new approaches to privacy and security measures should be tested before implementation and regularly reevaluated to assess the effect of these measures in real-world health care settings.

Our policy principles, along with our recommendations, call for the development of health information privacy and security protections that are comprehensive, transparent, understandable, adaptable, and enforceable. Any expanded federal data privacy framework should protect personal health information from unauthorized, discriminatory, deceptive, or harmful uses and align with the principles of medical ethics, respect individual rights, and support the culture of trust necessary to maintain and improve care delivery. It is equally vital that privacy guardrails be expanded and extended to entities not currently governed by privacy laws and regulations, which is the guiding rationale behind ADPPA.

THE NEED FOR A FEDERAL DATA PRIVACY FRAMEWORK

The United States does not have a comprehensive, national data privacy standard but instead relies on federal privacy statutes that are sector-specific and that establish varying degrees of protection. The most extensive privacy protections fall under HIPAA and address personal health information that is collected or held by HIPAA-covered entities (clinicians, health plans, health care clearinghouses) and their business associates and exchanged within traditional health care settings and operations. HIPAA does not address, nor could it have envisioned, the expanding ecosystem of non-covered entities collecting personal health information, including mobile health applications (mHealth apps), net search engines, large data brokers, and many others. This means that companies may generally collect, use, share, or sell data without having to notify the individuals to whom that data pertains.

A 2021 study by KPMG showed that 70 percent of companies increased their collection of personal consumer data despite 86 percent of consumers citing data privacy as a growing concern. Another study by the Pew Research Center indicated that half of American adults now say they have decided not to use a product or service due to worries over the use of their data. Data are also used in ways that disadvantage vulnerable communities and target people based on race, often with regard to eligibility for essential products and services such as home loans. These concerns have been further exacerbated by the ongoing COVID-19 pandemic with people fearing how their personal health data

are being shared for public health purposes. We are now seeing those fears heightened to an even greater extent for individuals seeking access to abortion services, which are no longer protected under federal law, but that often have a digital stamp forever linked to that care. According to the non-partisan Congressional Research Service (CRS), "various types of personal data—such as health records, financial records, geolocation information, and electronic communications—might shed light on an individual's abortion decision, and law enforcement could seek such information, either directly from the entity collecting the data or from another entity to whom the data has been shared or sold."

ACP'S HEALTH PRIVACY PRINCIPLES AND THE AMERICAN DATA PRIVACY AND PROTECTION ACT

We understand that ADPPA was designed with the intent of targeting big tech companies and their use or misuse of data/personal information and not necessarily targeting health care data, which has enjoyed robust privacy protections under HIPAA since 1996. That said, the policy reforms contained within ADPPA to non-HIPAA-covered entities are generally consistent with ACP's privacy principles, where applicable, and as outlined below. The legislation not only establishes a national data privacy standard, but it expands data privacy protections to entities (such as mHealth app developers) not subject to current privacy protections or regulations, both of which ACP strongly supports. It gives consumers various rights to access, correct, and delete their data held by ADPPA-covered entities. It also would require, absent a specific exception, that entities obtain a consumer's express affirmative consent before transferring their "sensitive covered data" (which includes, among other things, health information, geolocation information, and private communications) to a third party.

ACP Principle: **Protecting the privacy and security of personal health information collected both within and outside the health care system—while providing individual rights to that information—is essential for fostering trust in the evolving digital health care system, maintaining ethical standards and respect for persons, and promoting the safe delivery of health care.**

ACP calls for the same types of HIPAA protections for personal health information moving outside of traditional health care or when collected and used by entities not covered under existing HIPAA rules. Personal health information, as it moves through the health care system and as the digital health care ecosystem expands, requires responsible stewardship by all entrusted with it. Any federal data standard should provide persons the ability to know and control how their personal health information is accessed, used, and disclosed, as well as protect personal health information from unauthorized, discriminatory, deceptive, or harmful uses, and must apply to all entities not covered under existing law that collect, store, use, or exchange personal health information. As an example, ACP is greatly concerned that once information is disclosed to a health app, or other digital health tool, or other third-party applications or entities; it loses its HIPAA privacy protections, and that data could be used against patients and/or health care professionals when searching for and/or furnishing health services, including reproductive health services.

> **ADPPA:** The bill broadly defines covered data to include any information identifying, linked, or reasonably linkable to an individual or device linkable to an individual. We are pleased to see that ADPPA, as reported out of the Committee, identifies and expands the definition of covered "sensitive" data to include health, financial, biometric, genetic, race, color, ethnicity, religion,

internet browsing history over time, and precise geolocation information, among others, and is subject to heightened requirements. The bill's privacy protections would apply to most entities, including nonprofits, common carriers, and third parties that collect data through health apps. Some entities, such as those defined as large data holders that meet certain thresholds or service providers that use data on behalf of other covered entities, would face different or additional requirements.

ACP Principle: Increasing transparency and public understanding and improving models of consent about the collection, exchange, and use of personal health information within existing HIPAA rules as well as for entities collecting, exchanging, and using personal health information outside the health care system.

All entities that collect or use personal health information should provide standard and easily understandable notices of privacy practices, end-user licensing agreements, or terms of service to persons that contain the type of information collected, all allowable uses of information, and consent requirements. There should be a single, comprehensive taxonomy for consent provisions as well as standard structure for consent documents. Such consent models must account for literacy levels and preferred language, be revocable, and be unambiguous about which activities are permitted and which require consent. Within the guardrails of HIPAA and the health care system, permitted information-sharing activities requiring notice but not requiring consent must be narrowly defined, societally valuable activities of public health reporting, population health management, quality improvement, performance measurement, and clinical education.

ADPPA: The bill would require ADPPA-covered entities to disclose, among other things, the type of data they collect, what they use it for, how long they retain it, and whether they make the data accessible to the People's Republic of China, Russia, Iran, or North Korea. It would give consumers various rights over covered data, including the right to access, correct, and delete their data held by a particular covered entity. It would require covered entities to get a consumer's affirmative, express consent before using their "sensitive covered data" (defined by a list of sixteen different categories of data). It would further require ADPPA-covered entities to give consumers an opportunity to object before the entity transfers their data to a third party or targets advertising toward them. The bill also requires the Federal Trade Commission (FTC) to publish a public web page describing all provisions of the Act in plain language and advise individuals and ADPPA-covered entities of their rights and obligations under the Act. Covered entities must provide individuals with privacy policies detailing their data collection, processing, transfer, and security activities in a readily available and understandable manner. Privacy policies must be provided in all languages in which covered entities conduct business related to the covered data. Any material changes to a privacy policy require covered entities to notify individuals and provide an opportunity to withdraw consent before further processing the covered data of those individuals. The bill would also prohibit most ADPPA-covered entities from using covered data in a way that discriminates on the basis of protected characteristics (such as race, gender, or sexual orientation).

ACP Principle: **Believing that health IT and other digital technologies, including personalized digital health products, should incorporate privacy and security principles within their design as well as consistent data standards that support privacy and security policies and promote safety.**

Health IT and other digital technologies should incorporate audit trails to help detect inappropriate access to personal health information. Health IT and other digital technologies should facilitate the provision of useful and appropriate disclosure notifications to persons when personal health information is disclosed and for what purpose, with the ability to customize the types of disclosure notifications received. Efforts to develop a technical infrastructure allowing for automated and useful disclosure notifications and authorizations should be prioritized.

> **ADPPA**: Under the bill, ADPPA-covered entities have a duty to implement reasonable policies, practices, and procedures for collecting, processing, and transferring covered data. These correspond to the entity's size, complexity, activities related to covered data, the types and amount of covered data the entity engages with, and the cost of implementation compared to the risks posed. ADPPA requires large data holders that use algorithms to assess their algorithms annually and submit annual algorithmic impact assessments to the FTC. These assessments must describe steps the entity has taken or will take to mitigate potential harms from algorithms, including any harms specifically related to individuals under 17. These assessments must also seek to mitigate algorithmic harms related to advertising for housing, education, employment, healthcare, insurance, or credit, access to or restrictions on places of public accommodation, and any disparate impact on the basis of an individual's race, color, religion, national origin, gender, sexual orientation, or disability status. Algorithmic evaluations must occur at the design phase of an algorithm, including any training data that is used to develop the algorithm.

ACP Principle: **Supporting oversight and enforcement to ensure that all entities not currently subject to HIPAA rules and regulations and that interact with personal health information are held accountable for maintaining confidentiality, privacy, and security of that information.**

ACP supports oversight and enforcement to ensure that all entities not currently subject to HIPAA rules and regulations and that interact with personal health information are held accountable for maintaining confidentiality, privacy, and security of that information. Penalties for intentional or negligent breaches of privacy should be strictly enforced and state attorneys general should be empowered to enforce privacy rules. If state attorneys general do not pursue enforcement, there should exist a private right of action. Federal enforcement is needed when reidentification of deidentified personal health information occurs. Increased federal funding is necessary to support federal oversight and enforcement efforts that account for the additional entities engaging in personal health information collection exchange and use. It is critical that rules and enforcement efforts distinguish between inadvertent and intentional activities.

> **ADPPA:** The bill's provisions, as reported out of the Committee, would be enforceable by the FTC, under that agency's existing enforcement authorities, and by state attorneys general in civil actions. It would also create a delayed private right of action starting two years after the

law's enactment. Injured individuals would be able to sue covered entities in federal court for damages, injunctions, litigation costs, and attorneys' fees. Individuals would have to notify the FTC or their state attorney general before bringing suit. Before bringing a suit for injunctive relief or a suit against a small- or medium-size business, individuals would be required to give the violator an opportunity to address the violation. ADPPA would also generally preempt any state laws that are "covered by the provisions" of the ADPPA or its regulations, although it would expressly preserve nineteen different categories of state laws, including consumer protection laws of general applicability and data breach notification laws.

RECOMMENDATIONS

ACP does question whether ADPPA's provisions adequately protect an individual's personal data with respect to clinical research on human subjects and reproductive health information, including abortion-related services, which are no longer protected under federal law and have been criminalized in some states following the June 24, 2022, Supreme Court ruling striking down *Roe v. Wade*.

- **Research Data on Human Subjects**: The Committee-approved bill states, "A covered entity may collect, process, or transfer covered data for any of the following purposes if the collection, processing, or transfer is limited to what is reasonably necessary and proportionate to such purpose to conduct a public or peer-reviewed scientific, historical, or statistical research project that is in the public interest; and adheres to all relevant laws and regulations governing such research," [*including regulations for the protection of human subjects, or is excluded from criteria of the institutional review board*], as adopted by the Trahan/Bucshon amendment during the full Committee markup on July 20th.

  While ACP believes the Trahan/Bucshon amendment strengthened the base bill in helping to ensure privacy protections for research data on human subjects, we urge continued caution in this area in the interest of our patients. ACP policy states that each research subject or an authorized representative must be fully informed of the nature and risks of the research so that they may give informed consent to participate. Some groups may be more vulnerable to coercion or undue influence (such as children, prisoners, individuals with impaired decision-making capacity, and economically or educationally disadvantaged persons, as included in the Common Rule (i.e., Part 46 of Title 45 Code of Federal Regulations).

  While the Common Rule and some state laws have provisions regarding privacy and confidentiality requirements for research, the HIPAA Privacy Rule requires subject authorization for use or disclosure of protected health information for research. A privacy board can waive the authorization requirement or information can be used in a "limited data set" with a data use agreement or can be deidentified under HIPAA, although the HIPAA deidentification requirements are stricter than those under the Common Rule.

- **Reproductive Health Data**: The Committee-approved bill also states, "A covered entity may collect, process, or transfer covered data for any of the following purposes if the collection,

processing, or transfer is limited to what is reasonably necessary and proportionate to such purpose:

- To prevent, detect, protect against, or respond to fraud, harassment, or illegal activity. For purposes of this paragraph, the term "illegal activity" means a violation of a Federal, State, or local law punishable as a felony or misdemeanor that can directly harm.
- To comply with a legal obligation imposed by Federal, Tribal, local, or State law, or to investigate, establish, prepare for, exercise, or defend legal claims involving the covered entity or service provider.
- To prevent an individual, or group of individuals, from suffering harm where the covered entity or service provider believes in good faith that the individual, or group of individuals, is at risk of death, serious physical injury, or other serious health risk."

In many states, abortion bans include severe criminal penalties for patients and/or health care clinicians who perform or assist in the performing of abortion. In Texas, for example, the state's trigger law makes providing an abortion a first-degree felony, with physicians subject to punishments of life in prison and a $10,000 fine. Investigations threaten the patient-physician relationship as patients can be compelled to testify against physicians and vice versa and physicians will face criminal, civil, and/or professional penalties for providing evidence-based care. A 2021 report from the National Association of Criminal Defense Lawyers predicted that "a Supreme Court decision overturning *Roe v. Wade* will lead to rampant overcriminalization through regulatory enforcement and to mass incarceration on an unprecedented scale," as states dramatically expand the scope of criminal liability to cover patients, health care personnel, and others. With the Court having made such a decision, the criminalization of abortion services by states is expected to increase substantially and further subject health care professionals who provide such services as well as enablers and seekers of those services to prosecution.

As noted by CRS, existing privacy laws generally have law enforcement exceptions, which enable current-law covered entities to disclose, without consumer consent, data to law enforcement officials pursuant to a warrant, subpoena, or other legal process. In the case of reproductive health services, including abortion services in the post-*Roe* era, ACP is particularly concerned that this provision in ADPPA will allow, if not compel, entities to disclose private, digital information about an individual's efforts to obtain abortion-related services, which could then be used against that individual or their health care professional by law enforcement.

ACP strongly condemned the Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization* and issued a statement on June 24, 2022 to that effect. ACP believes in the principle of patient autonomy and ensuring access for all patients to the full range of reproductive health care services, including abortion, and believes that such reproductive health care decisions are foundational to the patient-physician relationship. A patient's decision about whether to continue a pregnancy should be a private decision made in consultation with a physician or other health care professional, without interference from the government.

CONCLUSION

We appreciate this opportunity to provide the clinician perspective on this important issue, and applaud the work being done on a bipartisan, bicameral basis to advance legislation establishing a federal data privacy framework, the ADPPA. We offer this feedback and our recommendations in the spirit of helping lawmakers bring this legislation to a vote for the greater benefit of our patients and consumers. If you have any questions regarding this letter, please do not hesitate to contact Jonni McCrann at jmccrann@acponline.org.

Sincerely,

Ryan D. Mire, MD, FACP
President

Cc: Chairs and Ranking Members, House Energy and Commerce Committee; Subcommittee on Consumer Protection and Commerce; Senate Committee on Commerce, Science, and Transportation