American College of Physicians
Leading Internal Medicine, Improving Lives

June 21, 2024

The Honorable Maria Cantwell
Chair
Commerce, Science & Transportation Committee
U.S. Senate
Washington, DC 20510

The Honorable Cathy McMorris Rodgers
Chair
Energy and Commerce Committee
U.S. House of Representatives
Washington, DC 20515

Dear Chairs Cantwell and Rodgers,

On behalf of the American College of Physicians (ACP), I write to commend your leadership and commitment to improving data privacy protections for all Americans with the introduction of the American Privacy Rights Act (APRA) draft legislation. ACP previously endorsed the American Data Privacy Protection Act (ADPPA), and we are pleased to see that APRA includes many of the provisions we support in the ADPPA. With the growing crisis around health information privacy, ACP appreciates the opportunity to offer a clinician perspective on this important bipartisan and bicameral draft legislation that would establish the nation's first comprehensive federal consumer data privacy framework, which has been an ACP priority for many years.

ACP is the largest medical specialty organization and the second-largest physician membership society in the United States. ACP members include 161,000 internal medicine physicians, 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.

Since the enactment of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), we have seen significant advancements in health care and information technology, including the use of personal health information (PHI) shared within non-HIPAA-covered entities. The changing ecosystem has led to the aggregation, commercialization, and weaponization of data, often without patients' awareness. We believe that as digital health technologies become ubiquitous and efforts continue to improve access to and interoperability of PHI, the privacy, security, disclosure, and use of patients' health data should remain at the forefront of our country's national agenda.

The Need for a Comprehensive Data Privacy Framework

The United States does not have a comprehensive, national data privacy standard but instead relies on sector-specific federal privacy statutes that establish varying degrees of protection. The most extensive privacy protections fall under HIPAA and address PHI 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. For non-HIPAA-covered entities such as mobile health applications (health apps), Internet search engines, and large data brokers, there are no laws that require them to notify app users when they collect, use, share, or sell app users' PHI data.

There is a growing consensus among American consumers that mobile apps are collecting too much personal consumer data. In fact, 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.

The United States needs to do better at protecting consumers' personal data, including PHI, and preventing companies from profiting from sharing the data with third parties for their own financial gain without consumers' consent and knowledge. With the changing digital health landscape, ACP is greatly concerned that once information is disclosed to a health app 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.

In ACP's health information privacy 2021 position paper, published in the *Annals of Internal Medicine*, ACP provides six key principles for health information privacy, protection, and use. These principles would improve privacy protections for PHI in the growing digital landscape. **ACP strongly supports the development and implementation of health information privacy and security protections that are comprehensive, transparent, understandable, adaptable, and enforceable. Further, any expanded federal data privacy framework should protect PHI from unauthorized, discriminatory, deceptive, or harmful uses. It is equally vital that privacy guardrails be expanded and extended to entities not currently governed by privacy laws and regulations.**

The American Privacy Rights Act (APRA)

While we understand that APRA's reach is broader than health care data, which has enjoyed robust privacy protections under HIPAA, the policy reforms within APRA for non-HIPAA-covered entities that gather PHI align with ACP's privacy principles. The draft legislation would not only establish a national data privacy standard, but it would also expand data privacy protections to entities that are not currently subject to HIPAA privacy protections or regulations, both of which ACP strongly supports. Further, it would give consumers various rights to access, correct, and delete their data and opt-out of targeted advertisement and data transfers. It would also 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. We

strongly support the draft legislation's prohibition on companies using consumers' personal data to discriminate or take adverse action against them. It would allow consumers to opt-out of allowing companies to use algorithms based on their personal data when they are making important life decisions such as those related to insurance, health care, housing, employment, and education. In ACP's recently published policy position paper on Artificial Intelligence in the Provision of Health Care, the College underscores our support for policies that would prohibit the use of algorithmic discrimination practices. Moreover, given the increase in data breaches over the last several years, we appreciate that this draft legislation contains provisions that would require companies to establish data security practices, assess systems' vulnerabilities, and avoid potential risks to consumer data.

Recommendations

The College offers the following recommendations that align with ACP's policy, to further strengthen the draft legislation.

- **Allow States to Further Protect their Residents**
  ACP supports a data privacy policy that would provide HIPAA protections for PHI moving outside of traditional health care environments or when collected and used by entities not covered under existing HIPAA rules. While we appreciate that APRA would provide a strong, comprehensive federal standard that states can adhere to, we support providing states with flexibility to further improve data privacy standards to fit their residents' needs. Because not all states have faced or will face the same threat of privacy violations or data breaches, they should not be constrained to a standard that may limit their ability to further protect their residents. **Thus, we urge you to consider ensuring that APRA will serve as a national standard for states to build upon based on each state's data privacy goals.**

- **Improve Transparency Practices for Research Data on Human Subjects**
  While we appreciate the draft legislation's intent 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 the 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 it can be deidentified under HIPAA, although the HIPAA deidentification requirements are stricter than those under the Common Rule. **We urge you to consider including a provision similar to the HIPAA Privacy Rule or Common Rule to improve confidentiality requirements for research data on human subjects.**

Conclusion

Once again, we applaud the work being done with APRA to advance legislation for a comprehensive federal data privacy framework. We offer this feedback in the spirit of helping lawmakers bring this legislation to a vote for the greater benefit of our patients and consumers. Should you have any questions, please contact Vy Oxman, Senior Associate of Legislative Affairs, at voxman@acponline.org.

Sincerely,

Isaac O. Opole, MBChB, PhD, MACP
President

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