AMERICAN ACADEMY OF FAMILY PHYSICIANS

September 28, 2023

The Honorable Bill Cassidy
Ranking Member
Senate Committee on Health, Education, Labor and Pensions
United States Senate
428 Dirksen Senate Office Building
Washington, D.C. 20510

Dear Ranking Member Cassidy:

On behalf of the American Academy of Family Physicians (AAFP), representing more than 129,600 family physicians and medical students across the country, I write in response your request for information (RFI) seeking feedback from health care stakeholders and to provide the family medicine perspective on ways to leverage technology to improve patient care, while safeguarding the privacy of patient data.

This RFI centers on the privacy, security, use, and transfer of patient and consumer health data in the ecosystem outside of the Health Insurance Portability and Accountability Act (HIPAA), where it is largely unprotected by federal laws or regulations and which has been a growing concern for the AAFP. The opening of your letter acknowledges that safeguarding patient privacy is an essential element in building trust in our health care system. The AAFP wholeheartedly agrees.

We have long supported policies that guarantee the appropriate security of protected health information while working to improve patients' access to their data, as well as the ability to share patients' health information across the care team. We are strongly supportive of making data reliably interoperable while maintaining patient confidentiality and the fundamental right to privacy. A confidential relationship between physician and patient is essential for the free flow of information necessary for sound medical care, and confidentiality of patient health data should continue to be a priority outside of the patient-physician relationship. We acknowledge that ensuring health data privacy long-term is going to require a federal citizen data privacy law and regulatory framework. In response to some of the specific questions and broader categories presented in the RFI, the Academy offers the following responses:

General Privacy Questions:

1. *What is health data? Is health data only data governed by HIPAA, or are there other types of health data not governed by HIPAA? Should different types of health data be treated differently? If so, which? How? If not, why not?*

AAFP Response:

Health data can be defined as data used by patients and their caregivers to help maintain a person's health or treat disease. With this broad definition, not all health data is governed by HIPAA. HIPAA's

approach is to define health data as patient data generated or maintained by a covered entity. While clinicians and health care organizations must follow the HIPAA Privacy Rule, which guards against disclosures of protected health information (PHI), other entities and data that do not qualify as PHI are not bound by the same rules. For example, a "personal health record" (PHR) is an electronic health record that can be drawn from multiple sources and that is managed, shared, and controlled by or primarily for a patient. This is separate from a physician or hospital's electronic health record (EHR) system, which is required to follow the HIPAA Privacy Rule and primarily controlled by the health system.

Today, patients have health data that is not confined to covered entities. This broad definition makes it difficult to create a dichotomy between health data and non-health data, as it depends if the data is used for health. For example, geolocation data from a mobile device could be used to help remind patients about healthier food choices, such as when they are located within a fast-food establishment. These data could also help identify community services on their route to home or work. In these examples, that data could fit within the definition of health data, but not all geolocation data would be considered health data.

One way that existing policies have been constructed to limit data is to focus on sensitive data, such as certain diagnosis, medications, and tests that have historically been stigmatized (i.e. HIV status, mental illness, and substance use). However, this restricts safeguards to a very small subset of health data. Additionally, the privacy preferences of individuals vary, which would make it difficult to establish a universal "sensitive" health data definition.

The AAFP believes that patients should have the right to privacy for all their health data regardless of the entity creating or maintaining the information. At the same time, it is critical that we do not put additional burdens on physician practices and hospitals, which could have significant consequences such as taxing primary care further and stifling health information exchange. The nation has worked hard over the last few decades to enable continuity of care through health data sharing, which the potential to improve patient health outcomes and reduce cost savings. Federal policymakers must ensure we do not undermine that progress and continue to support the vital exchange of health information in any efforts to better govern health data and protect patients' privacy.

HIPAA should be left in place for covered entities, as they have a long track record of protecting health information. Within covered entities, the lack of or inability to promote information exchange would have the greatest negative impact on patients. We believe additional safeguards for non-covered entities should be created.

2. *Which entities outside of HIPAA Covered Entities should be accountable for the handling of health data (not necessarily HIPAA-covered data)? Should different types of entities have different obligations and privileges? Please explain using examples.*

AAFP Response:

The Academy believes that any entities that create, store, organize, manage, or transfer health data should be accountable for maintaining patient privacy and confidentiality. As noted in our above response and examples, non-clinician or health care entities and data that do not qualify as PHI are not bound by the same rules as HIPAA-covered entities. Congress has recognized that PHR vendors and PHR related entities—companies that offer services related to, access information in, or send information to PHRs—were collecting consumers' health information but were not subject to the privacy and security requirements of HIPAA. Large technology companies and data brokers can obtain and inappropriately use extremely detailed information about individuals, including internet

search histories, communications, finances, and location data. These companies may also require the surveillance of personal information as a condition of use for apps individuals use to access their health data or improve their health.

There should be a minimum standard that all entities must comply with. Additionally, any entity that receives patient data from a covered entity should be required to comply with the requirements of the HIPAA privacy and security rules. This is currently enforced through Business Associate Agreements (BAA), but if a patient extracts their health information from a covered entity, the BAA does not apply to the entity that the patient gives their health data to. **The AAFP urges that this loophole be closed.** This could also be a way to constrain the definition of health data to a manageable level in our current technology environment.

Health Information Under HIPAA

1. *How well is the HIPAA framework working? What could be improved?*

AAFP Response:

The basic framework of the HIPAA privacy and security rules are working. However, there is a need to modernize the language of the existing rules to better align with today's technological landscape. Additionally, the AAFP believes greater clarity is needed to describe how HIPAA and other newer regulations, such as the information blocking provisions in the Cures Act Final Rule, work together. There is likely additional opportunity to streamline the rules to decrease administrative burden on covered entities, including family physicians.

2. *Should Congress update HIPAA?*

AAFP Response:

As noted previously, the AAFP believes there is a need to modernize HIPAA to better reflect and account for our current health technology landscape. For example, the Academy recently commented on a proposed rule from the Department of Health and Human Services (HHS) seeking to increase protections for certain highly sensitive PHI and provided our feedback on ways to strength and update HIPAA accordingly.

3. *Should Congress expand the scope of HIPAA? What specific information should be included in the HIPAA framework?*

AAFP Response:

The AAFP believes that the current scope of HIPAA is appropriate. Instead, we recommend that Congress create a new set of requirements for non-covered entities that is harmonized with the HIPAA requirements.

Collection of Health Data:

In general, the collection of health data should be consent-based with patients providing their explicit authorization, and there should be transparency of how the data will be used in clear, plain language.

AAFP policy prescribes that electronic health information communication systems must be equipped with appropriate safeguards (e.g., encryption, message authentication, user verification, etc.) to protect physician and patient privacy and confidentiality. Individuals and entities with access to these

electronic systems outside of the patient-physician relationship should be subject to clear, explicit, mandatory policies and procedures regarding the entry, management, storage, transmission, and distribution of patient and physician information.

Financial Information:

1. *How should financial information for health care services not covered by HIPAA (i.e., claims data, billing) be treated?*

If financial information for health care services not covered by HIPAA is tied to the description of the service or organization, then the Academy believes it should be considered health data and treated as such.

Sharing of Health Data:

We acknowledge the complexity and nuances of collecting health data outside of the HIPAA framework. The AAFP believes that patients should control when and where their PHI is shared. However, sharing of health data can drive learning and new discoveries within health care research and the medical community. Requiring all de-identified health data to be opt-in would limit the volume of data available, even if many patients would be comfortable with that use of their data. Congress should consider the value of having the sharing of sensitive health data (if identifiable) be opt-in, and the sharing of all other health data be opt-out.

The AAFP's policy on data stewardship—which addresses how de-identified clinical and administrative data derived from electronic health records (EHRs) are collected and used by third parties—states that submission of data from physician practices to third parties must be voluntary, third parties must provide written policies detailing the intended uses of such data, and data storage must adhere to industry and regulatory standards for confidentiality. We believe this should be reflected in any federal efforts to improve data privacy.

Congress should also protect against the unwarranted and unconsented sale and transfer of personal and health information that exists outside of HIPAA. The AAFP has previously endorsed federal legislation that would prohibit data brokers from selling and transferring customers' health and location data and requires the Federal Trade Commission to promulgate rules to implement and enforce these protections. We believe such measures should be a part of any comprehensive federal legislation to address consumer data privacy.

Artificial Intelligence:

The family medicine experience is based on a deeply personal patient-physician interaction that requires support from technology, including artificial intelligence (AI). AI and machine learning (AI/ML) systems have the potential to bolster family medicine by supporting the four C's of primary care (first contact, comprehensiveness, continuity, and coordination of care), enhancing capacity, and extending capabilities. AI/ML can be leveraged to help achieve this quintuple aim if applied appropriately in family medicine. To that end, the AAFP believes that AI/ML based solutions should adhere to a set of principles that can help ensure the appropriate application of AI/ML in family medicine.

The issue of sharing health data certainly applies to AI/ML, and AI/ML should be evaluated with the same rigor as any other tool utilized in health care. In the initial set of principles put forth by the AAFP, we include:

5. **Respect the Privacy of Patients and Users:** AI/ML requires large volumes of data for training. It is critical for patients and physicians to trust companies will maintain confidentiality of data from them. Companies must provide clear policies around how they collect, store, use, and share data from patients and end-users. Companies must get consent for collecting any identifiable data, and the consent should clearly state how the data will be used or shared.

Considerations should also be given to the potential for AI to identify patients from data thought to be unidentifiable and how to address these privacy concerns.

State and International Privacy Frameworks:

Data sharing is difficult, particularly across state lines given differing state patient privacy and confidentiality requirements. The current heterogeneous nature of state laws has limited interoperability across clinicians and other health care entities while increasing the cost of health care through administrative burden and duplicative paperwork, tests, and other services. Therefore, a national data privacy framework could help. The AAFP believes that federal legislators should seek a greater degree of standardization by recognizing the following principles regarding the privacy of medical information:

A. The right to privacy is personal and fundamental.

B. Medical information maintained by physicians is privileged and should remain confidential.

C. The patient should have a right of access to his/her medical records and be allowed to provide identifiable additional comments or corrections. The right of access is not absolute. For example, in rare cases where full and direct disclosure to the patient might harm the patient's mental and/or physical well-being, access may be extended to his/her designated representative, preferably a physician.

D. Medical information may have legitimate purposes outside of the physician/patient relationship, such as billing, quality improvement, quality assurance, population-based care, patient safety, etc. However, patients and physicians must authorize release of any personally identifiable information to other parties. Third party payer and self-insured employer policies and contracts should explicitly describe the patient information that may be released, the purpose of the information release, the party who will receive the information, and the time period limit for release. Policies and contracts should further prohibit secondary information release without specific patient and physician authorization.

E. Any disclosure of medical record information should be limited to information necessary to accomplish the purpose for which disclosure is made. Physicians should be particularly careful to release only necessary and pertinent information when potentially inappropriate requests (e.g., "send photocopies of last five years of records") are received. Sensitive or privileged information may be excluded at the option of the physician unless the patient provides specific authorization for release. Duplication of the medical record by mechanical, digital, or other methods should not be allowed without the specific approval of the physician, taking into consideration applicable law.

F. Disclosure may be made for use in conducting legal medical records audits provided that stringent safeguards to prevent release of individually identifiable information are maintained.

Enforcement:

2. *OCR has primary authority over enforcement of HIPAA. However, other federal agencies such as the Federal Trade Commission (FTC) have oversight of certain health data that can implicate HIPAA. To what extent should these agencies have a role in the safeguarding of health data? What duplication or conflict currently exists between how different agencies enforce violations of health laws?*

The FTC's authority to police "unfair and deceptive" practices is key to preventing vendors and data brokers from inappropriately using PHR identifiable health information. In August, the AAFP submitted comments on the FTC's proposed rule to amend the Health Breach Notification Rule (HBNR) that supported the agency's step to clarify for organizations not covered by HIPAA exactly how they are required to notify customers, the FTC, and, in some cases, the media if there's a breach of unsecured, individually identifiable health information. However, **Congress can take further action to provide greater, clearer enforcement authority to the FTC and other federal agencies with appropriate jurisdiction to better protect the privacy of patients' health data.**

Thank you for the opportunity to share the family physician perspective and offer this feedback on leveraging technology to improve patient care, while safeguarding the privacy of patient data. Should you have any questions, please contact Natalie Williams, Senior Manager of Legislative Affairs at nwilliams2@aafp.org.

Sincerely,

Sterling N. Ransone, Jr. MD FAAFP

Sterling N. Ransone, Jr., MD, FAAFP
Board Chair, American Academy of Family Physicians