AMERICAN ACADEMY OF FAMILY PHYSICIANS

September 15, 2022

The Honorable Frank Pallone
Chairman
Committee on Energy & Commerce
U.S. House of Representatives
Washington, D.C. 20515

The Honorable Cathy McMorris Rodgers
Ranking Member
Committee on Energy & Commerce
U.S. House of Representatives
Washington, D.C. 20515

Dear Chairman Pallone and Ranking Member McMorris Rodgers:

On behalf of the American Academy of Family Physicians (AAFP) and the 127,600 family physicians and medical students across the country we represent, I write to express our appreciation for your interest in promoting and protecting data privacy.

Effective data sharing is difficult, particularly across state lines given different state privacy and confidentiality requirements. The AAFP is particularly concerned about 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. **We believe federal legislation is necessary to achieve a greater degree of data standardization and adherence to agreed-upon principles related to the privacy of health data.**

The AAFP has 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 physician-patient relationship.

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

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 practice 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 national data privacy framework.

1133 CONNECTICUT AVE., N.W., STE. 1100 | WASHINGTON, DC 20036-4305 | (800) 794-7481 | (202) 232-9033

Maintaining an up-to-date and robust cybersecurity footing can be an overwhelming task for some covered entities, especially small and medium physician practices. Any national data privacy legislation with new requirements must avoid imposing excessive administrative burden, liability for data breaches of third-party apps and application programming interfaces (APIs), or additional expenses to implement safeguards or contract with EHRs on physicians.

Even though a physician may not be subject to costly HIPAA breach penalties as a result of breaches of medical records due to vulnerabilities in third-party APIs and apps, they would still incur significant damage to their reputation and patient-physician trust, from a perceived mishandling of patient data. Additionally, relying on a patient's clinician to determine whether an app that the patient wishes to use or the clinician wishes to recommend has appropriate security (and privacy) places a significant burden on individuals and physician practices, who are likely unequipped to make this determination or provide patient education on app security.

While clinicians and health care organizations must follow the HIPAA Privacy Rule, which protects against disclosures of protected health information (PHI), other entities and data that do not qualify as PHI are not bound by the same rules. Large technology companies and data brokers could 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.

Federal legislation to establish a national data privacy framework must protect against the unwarranted and unconsented sale and transfer of personal and health information that exists outside of HIPAA. The AAFP has endorsed the Health and Location Data Protection Act (S. 4408), which prohibits 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 legislation to address consumer data privacy and are especially timely given patient privacy concerns that have arisen in the wake of the Supreme Court's *Dobbs* decision.

Thank you again for your work toward establishing a national framework to protect consumers' data, specifically health and personal identifiable data outside of HIPAA. We are eager to remain engaged with the Energy and Commerce Committee on this important issue as the American Data Privacy and Protection Act and other legislation advances. If you have any questions, please contact Erica Cischke, Director of Legislative and Regulatory Affairs, at ecischke@aafp.org.

Sincerely,

Ada D. Stewart, MD, FAAFP
Board Chair, American Academy of Family Physicians