COLLEGE of AMERICAN PATHOLOGISTS

April 7, 2025

The Honorable John Joyce, M.D.
Vice Chairman
House Committee on Energy and Commerce
Washington, D.C. 20515

CC: Representatives Morgan Griffith, Troy Balderson, Jay Obernolte, Russell Fry, Nick Langworthy, Tom Kean, Craig Goldman, and Julie Fedorchak

Re: Privacy Working Group Request for Information

Sent to: PrivacyWorkingGroup@mail.house.gov

Dear Vice Chairman Joyce,

As the world's largest organization of board-certified pathologists and leading provider of laboratory accreditation and proficiency testing programs, the College of American Pathologists (CAP) serves patients, pathologists, and the public by fostering and advocating excellence in the practice of pathology and laboratory medicine worldwide. As physicians specializing in the diagnosis of disease through laboratory methods, pathologists have a long track record of delivering high quality diagnostic services to patients and other physicians.

The CAP is deeply concerned that our nation's health care information technology system is woefully unprepared for the threat that cybersecurity attacks pose. As a result, we consider these attacks to be a major threat to patient safety. Last year, many of our CAP members experienced significant cyberattacks in their health care organizations that delayed and disrupted patient care delivery and threatened patient safety. Physicians were locked out of treatment tools and health information technology (HIT) systems, preventing them from looking up patients' past medical history, test results, and other essential data, and interfering with communication with colleagues. Further, hospital equipment they use for care was shut down, creating backlogs that further delayed treatment. We learned, unfortunately, that hospital mortality rises in the aftermath of a cyberattack. Additionally, health care providers face financial burdens with disrupted and uncertain payment processing. Cybersecurity consultants and government officials have consistently identified the health care sector as the sector of the U.S. economy most susceptible to cyberattacks.

Pathologists serve in a unique role that bridges health care systems as directors of clinical laboratories that are certified through the Clinical Laboratory Improvement Amendments (CLIA). In this capacity, they oversee complex information technology systems that operate within a laboratory. Patient data and test results are recorded in the laboratory information system (LIS), which is often separate from the electronic health record (EHR) system. Pathologists often have limited knowledge

College of American Pathologists
1001 G Street, NW, Suite 425W
Washington, DC 20001
202-354-7100

of and authority over how laboratory data is incorporated into an EHR system or used by other clinical decision support software. Consequently, cybersecurity has significant implications for pathologists and clinical laboratories.

Stakeholders in health care delivery are insufficiently prepared to meet the cybersecurity challenges of an increasingly digital system which exchanges more electronically stored patient information, both medical and financial, than ever before. Increasing cyberattacks in the health care sector can compromise both sensitive patient information and financial data. This has national security implications, as adversary countries could exploit such sensitive data to cause serious harm to the U.S. Despite health care organizations purchasing cyber insurance, insurers are imposing more rigorous terms and conditions with increasing premiums. The magnitude of the challenge in coordinating stakeholders across the entire health care system and in ensuring patient safety and access to care in the aftermath of a cybersecurity incident necessitates federal leadership, guidance, and financial support. Any federal legislation should be carefully crafted with stakeholder input to ensure that these nuances are accounted for.

The CAP appreciates the opportunity to share our views with the Privacy Working Group regarding federal comprehensive data privacy and security standards, particularly as it pertains to patient protections in the health care sector. We reviewed the questions for consideration provided by the Working Group and have provided responses to several of these questions as noted below. In sum, the CAP believes the intended outcome of any cybersecurity measure must be protection of patient care and patient data.

I. Roles and Responsibilities

A. How can a federal comprehensive data privacy and security law account for different roles in the digital economy (e.g., controllers, processors, and third parties) in a way that effectively protects consumers?

To effectively protect consumers, a federal comprehensive data privacy and security law should account for different roles in the health ecosystem by assigning distinct cybersecurity responsibilities for those differing roles. For example, physicians and other health care professionals have a different role to play in health care delivery than insurers and health plans. Physicians rely on robust information to deliver high-quality health care services. Consequently, physicians should be subject to cybersecurity responsibilities that reflect their unique role.

Further, a federal comprehensive data privacy and security law—or more generally, the federal government's cybersecurity infrastructure—should provide incentives and educational resources to best equip physicians and other health care providers for following protections for the sensitive data that they use on behalf of patients to deliver high-quality health care services.

B. What are appropriate obligations for different regulated entities, and what are the practical and legal limitations associated with each type of entity?

In the aftermath of a cyberattack, federal data privacy and security law must assign appropriate obligations based on the roles that different stakeholders play. That is, any cybersecurity infrastructure that is implemented through a federal comprehensive data privacy and security law should protect physicians and other health care providers from cybersecurity risks outside of their control (e.g., risks from third-party vendors, clearinghouses, etc.). For example, once data leaves the laboratory HIT infrastructure, the laboratory often does not have control over how another HIT system uses the data. Moreover, when a cyberattack occurs on a non-laboratory system, the patient data breach is outside the laboratory's control. The hacked entity should bear the responsibility for reporting the breach to patients and addressing any problems that arise.

C. Should a comprehensive data privacy and security law take into consideration an entity's size, and any accompanying protections, exclusions, or obligations?

A comprehensive federal data privacy and security law should use a risk-based framework to assign cybersecurity responsibilities and requirements on health care entities. That is, different entities should have different cybersecurity responsibilities and different cybersecurity requirements based on differences in risk.

Risk should be defined not only in terms of an entity's size and the number of patients that entity affects but also the risk the entity poses to the entire health system. For example, when a large corporate entity that touches many different entities is hacked, the effects of that hack often reverberate across the entire U.S. health system. The same would not be true if a small rural private practice is hacked. Consequentially, a large entity should have more substantial cybersecurity responsibilities than a small, more isolated entity because the consequences of a cyberattack on a large corporate entity are more devastating.

To summarize, a comprehensive data privacy and security law should take into consideration an entity's size, reach, and downstream impact when assigning protections, exclusions, or obligations.

II. Personal Information, Transparency, and Consumer Rights

A. Please describe the appropriate scope of such a law, including definitions of "personal information" and "sensitive personal information."

For health care information, the Health Insurance Portability and Accountability Act (HIPAA) already sets sufficient definitions for health care data. Any cybersecurity law related to health care information should be addressed through HIPAA, rather than adding further requirements or duplicative layers of statute.

B. What disclosures should consumers be provided with regard to the collection, processing, and transfer of their personal information and sensitive personal information?

For health care information, HIPAA includes appropriate disclosure requirements.

C. Please identify consumer protections that should be included in a comprehensive data privacy and security law. What considerations are relevant to how consumers enforce these protections and how businesses comply with related requirements?

For health care information, HIPAA addresses protections and compliance requirements.

D. What heightened protections should attach to the collection, processing, and transfer of sensitive personal information?

For health care information, HIPAA addresses protections and compliance requirements.

III. Existing Privacy Frameworks & Protections

A. Please provide any insights learned from existing comprehensive data privacy and security laws that may be relevant to the working group's efforts, including these frameworks' efficacy at protecting consumers and impacts on both data-driven innovation and small businesses.

Physician practices and hospitals have experienced several major data breaches during the past year. The disruptions in electronic health care transactions (including claims processing, eligibility verification, and electronic prescribing) were lengthy and very disruptive. The CAP is recommending a tiered, risk-based structure because of these experiences.

College of American Pathologists
1001 G Street, NW, Suite 425W
Washington, DC 20001
202-354-7100

B. Please describe the degree to which U.S. privacy protections are fragmented at the state-level and the costs associated with fragmentation, including uneven rights for consumers and costs to businesses and innovators.

The vast array of state laws pertaining to the handling of health information makes it difficult for businesses and innovators to catalogue and comply with all 50 states' laws, particularly when disclosing health information across state lines. Many physicians and other health care providers, such as laboratories, and other stakeholders operate in multiple states, which causes compliance difficulties when state laws vary.

D. How should a federal comprehensive privacy law account for existing federal and state sectoral laws (e.g., HIPAA, FCRA, GLBA, COPPA)?

We support setting a national standard for privacy law. We want to ensure that any federal comprehensive privacy law does not supersede, duplicate, or contradict HIPAA for the health care sector. HIPAA establishes national standards to protect individuals' electronic personal health information that is created, received, used, or maintained by a covered entity, which includes health plans, clearinghouses, and physicians and other health care providers. It requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. Any issues with privacy in health care should be dealt with by amending HIPAA, not adding further requirements or layers of statute.

Federal agencies should develop consistent and coordinated cybersecurity requirements. The agencies should develop the regulations with notice-and-comment rulemaking to ensure the opportunity for involvement of stakeholders from across the health care system to ensure that requirements can be practicably implemented.

IV. Data Security

A. How can such a law improve data security for consumers? What are appropriate requirements to place on regulated entities?

Cybersecurity protections are beneficial for patients, physicians, and all stakeholders in health care delivery, and they help guard our national security. The federal government should require that regulated entities maintain standards to protect health care data, help prevent cyberattacks, respond in the event of such an attack,

and help mitigate any downstream repercussions to other entities indirectly impacted by the attack.

In the wake of attacks on non-provider entities within the last year, physicians and other health care providers experienced significant delays in claims processing and payment, in some cases jeopardizing the financial survival of some physician practices. These delays can also have significant implications for patient cost sharing. Patients and providers should have protections against the problems that occur when breaches result in delayed payment processing.

V. Artificial Intelligence

A. How should a federal comprehensive data privacy and security law account for state-level AI frameworks, including requirements related to automated decision-making?

We are concerned about the burdens of following different state-level frameworks. A federal comprehensive data privacy and security law provides the opportunity to set the national standard.

VI. Accountability & Enforcement

A. Please identify the benefits and costs of expert agencies retaining sole authority to enforce a federal comprehensive data privacy and security law.

Having an expert agency retain sole authority will help physicians and other health care providers understand clear expectations from an authoritative source.

VII. Additional Information

The federal government's role in cybersecurity protections for healthcare should be to set up a risk-based cybersecurity infrastructure, provide incentives for the health care industry to set up cybersecurity protections, and provide resources to assist with recovery from a cyberattack. In the creation of this risk-based cybersecurity infrastructure, the federal government should incentivize adoption and implementation of cybersecurity protection by health care entities. Incentives should include financial assistance from federal agencies, such as grants and increased federal health care program payments, for steps taken to improve cyberattack prevention and response. A lack of incentives from the federal government would make any regulatory requirements on cybersecurity and privacy amount to a burdensome unfunded mandate, which would be exacerbated by the increasing costs of cyber insurance that more health care organizations are purchasing.

College of American Pathologists
1001 G Street, NW, Suite 425W
Washington, DC 20001
202-354-7100

As the infrastructure for cybersecurity protection is being built and constantly changing, the federal government's adoption and implementation approach should not be punitive; rather, it should enable physicians and other health care providers to demonstrate that they are meeting recommended standards. Federal oversight agencies could help facilitate this by providing educational resources and guidance to enable entities to demonstrate that they are following optimal approaches to address an evolving landscape of cybersecurity.

Additionally, the federal government should rigorously review and scrutinize any proposed health care mergers in light of the increased cybersecurity risk to determine their effects on patients, physicians, and other health care providers. As stated previously, any law passed should take into consideration an entity's size, reach, and downstream impact when assigning protections, exclusions, or obligations. Protections must also be in place to ensure consolidated entities are not permitted to profit in the aftermath of cybersecurity attacks.

Finally, in the event of a cyberattack, the federal government and private payers should provide continued reimbursement to practices for health care services provided. In addition, when normal operations have resumed, physicians and other health care providers must have protection for unpaid claims that could not be paid/submitted earlier. Previously submitted claims should be paid back over time and not in lump sums.

The CAP appreciates the Committee and Working Group's efforts in this space. We look forward to working with you on federal comprehensive data privacy and security standards. Please contact Hannah Burriss at hburris@cap.org if you have any questions regarding these comments.

Sincerely,

Donald S. Karcher, MD, FCAP
President

College of American Pathologists
1001 G Street, NW, Suite 425W
Washington, DC 20001
202-354-7100