MPL | MEDICAL PROFESSIONAL LIABILITY ASSOCIATION

April 7, 2025

The Hon. Brett Guthrie, Chair
Committee on Energy and Commerce
United States House of Representatives
2125 Rayburn House Office Building
Washington, DC 20515

The Hon. John Joyce, M.D., Vice Chair
Committee on Energy and Commerce
United States House of Representatives
152 Cannon House Office Building
Washington, DC 20515

Subject: Data Privacy Working Group

Dear Chairman Guthrie and Vice Chairman Joyce:

On behalf of the Medical Professional Liability (MPL) Association and its members which insure approximately one million healthcare professionals and ten thousand hospitals and facilities throughout the United States, I would like to express our appreciation for your request for stakeholder input to the recently formed data privacy working group.

The MPL Association supports the adoption of federal consumer data privacy and security measures that enhance transparency and protections related to consumers' personal information. We believe such protections, however, must also allow for flexibility for covered entities based on their size and available financial resources of covered entities. We also believe that these proposals should factor in the nature, scope, and complexity of an entity's activities in handling consumer data, including recognizing the legitimate need for companies to use consumer data for appropriate business purposes. Such purposes include the provision of a full range of insurance services to meet their contractual obligations, the analysis of data to enhance future business practices, and compliance with all legal requirements. In this regard, it is vital to consider the unique circumstances which MPL insurers face on all these fronts. With this in mind, we strongly recommend that Congress adopt the following principles as it develops federal data privacy legislation.

Federal Preemption

First and foremost, any legislation considered by Congress must include complete preemption of current, or future, state data privacy/security requirements. Insurers already face not just a myriad of sometimes conflicting or overlapping state laws on data privacy aimed at the broader business community, they also must deal with unique laws specifically targeting the insurance industry. A federal statute must create one uniform standard to allow businesses involved in multi-state activities to comply with only one set of rules. Retention of current state laws or even certain aspects of some state laws will only make compliance more difficult and needlessly burdensome on the business community.

Conflict with Existing Federal Statutes

It is also vitally important that new data privacy protections not conflict with those protections already contained in federal statute. Specifically, entities that already comply with the Health Insurance Portability and Accountability Act (HIPAA), the Health Information Technology for Economic and Clinical Health Act (HITECH), and the Gramm-Leach-Bliley Act should be exempted from compliance with a new data privacy law.

Limitations on Processing of Covered Information

As previously stated, MPL insurers collect and retain personal information about consumers for claims handling, long-term underwriting, risk management, and quality improvement/patient safety purposes. Consequently, any effort to limit the processing or retention of covered information, including personal health information, should be accompanied by an exception for the lawful, internal use of covered information by a covered entity so long as the entity can demonstrate it is using the data for purposes reasonably related to the reason the data was collected.

Flexibility

To the extent that future legislation requires entities to develop certain policies, practices, or procedures pertaining to data privacy, such matters should reflect the relevance of those issues to the businesses and transactions in question. Specifically, to prevent overburdening smaller businesses or those with limited collection of data, requirements should be adaptable based on the size of the entity involved, the nature of the data it collects, and the cost of implementing protections in relation to the potential risks involved.

Limit Consumers' Ability to Delete/Change Data

Given the "long-tail" nature of MPL insurance, our member companies must collect and retain accurate information about parties (i.e., personal health information) to an MPL claim for claims processing, risk management, and quality improvement/patient safety purposes. Hence, the establishment of a consumer right to delete or correct information should be accompanied by exceptions that allow a covered entity to deny such requests with an explanation of its need to retain accurate information to fulfill legitimate business transactions and comply with legal obligations.

Enforcement

Federal legislation will clearly require some form of enforcement mechanism in order to ensure compliance. In this regard, we strongly recommend that enforcement be addressed by the appropriate state entity, and not via the creation of a new federal bureaucracy. Doing so will allow enforcement to be handled by agencies most familiar and involved with the affected parties, thus allowing for more productive application of the law. That said, the states' ability to act should be carefully constrained to ensure abusive enforcement actions are not taken. In this regard, we strongly oppose any use of private rights of action as an enforcement mechanism. Such actions, whether authorized in a federal data privacy law or allowed to be set in state law, will serve only to clog the courts with needless litigation and divert needed resources from data protection to litigation. Enforcement would be better

and more efficiently achieved if done via civil penalties or injunctive relief for covered entities that fail to comply. In addition, penalties should be implemented on a tiered basis based on an entity's past behavior, previous corrective actions taken, and the seriousness of the infringement. In addition, any penalties issued to an entity should be used solely to compensate those who were actually harmed by the data breach and to offset any enforcement costs. Under no circumstances should enforcement entities be authorized to turn civil penalty funds over to outside interest groups.

Third Parties

It is wholly appropriate for federal law to require that entities covered under such law require third parties with which they may contract to provide the same level of data protection they are required to provide. Such a requirement should be fulfilled by mandating that third parties contractually commit to such arrangements. It would be inappropriate, however, to require the covered entity to be held liable for whether the third party upholds its contractual obligations. In addition, any requirement that covered entities enter into such contacts with third-party vendors should be implemented over time, so as not to require an immediate, wholesale re-writing of all of a covered entity's third-party contracts. We recommend a grace period of two years.

Transparency

A previous congressional proposal required a covered entity to annually disclose, to a federal regulatory agency, what type of consumer information it collects and how it utilizes and safeguards this information on a periodic basis. That approach was overly bureaucratic and posed a significant financial and human resource burden on covered entities, including our member companies. Instead, it should be sufficient for covered entities to attest that they comply with any requirements put forward by the relevant regulatory entity.

In closing, the MPL Association appreciates this opportunity to provide input as the Energy & Commerce Committee's data privacy working group proceeds with its efforts to develop a workable federal data privacy law. Please do not hesitate to contact me at 240.813.6139 or via email at mstinson@MPLassociation.org should you have any questions or need any further information.

Sincerely,

Michael C. Stinson
Vice President, Public Policy and Legal Affairs