March 17, 2017

The Honorable Raymond G. Farmer, Chair
The Honorable Elizabeth K. Dwyer, Vice Chair
Cybersecurity (EX) Working Group
National Association of Insurance Commissioners
1100 Walnut Street, Suite 1500
Kansas City, MO 64106-2197

ATTN: Sara Robben, NAIC Statistical Advisor
Via email: srobben@naic.org

Subject: Third Draft of Insurance Data Security Act

Dear Director Farmer and Superintendent Dwyer:

On behalf of PIAA and the medical/healthcare professional liability (MPL/HPL) community, I would like to thank the Cybersecurity (EX) Task Force for giving us another opportunity to share our perspective on the potential impact of the Insurance Data Security Act on the MPL insurance industry.

PIAA is the insurance industry trade association that represents a full range of entities doing business in the MPL/HPL arena, including insurance companies, risk retention groups, captives, trusts, and other entities. PIAA members include MPL/HPL enterprises owned and/or operated by physicians, hospitals, health systems, dentists and oral maxillofacial surgeons, podiatrists, chiropractors, and healthcare providers such as nurse practitioners, nurse midwives, CRNAs, and many others, as well as insurance carriers with a substantial commitment to the MPL/HPL line. PIAA members insure more than two-thirds of America's physicians in private practice, as well as dentists, nurses and nurse practitioners, and other healthcare providers, and they insure more than 2,500 hospitals nationwide.

PIAA shares the NAIC’s interest in balancing the need for appropriate levels of security for consumers’ personal information with the need to adopt flexible data security and breach response measures that are responsive to insurers’ circumstances. While the third draft of the model act includes some welcome changes, we believe that additional changes are necessary for this model law to achieve a truly balanced approach. Below, please find additional feedback for the task force’s consideration.

Section 2. Purpose and Intent

Section 2 establishes a safe harbor for licensees, such as MPL/HPL insurers, that are required to establish and maintain safeguards for personal health information (PHI) under the Health Insurance Portability and Accountability Act (HIPAA). While PIAA appreciates the task force’s effort to minimize duplicative breach notification requirements, we would prefer for the task force to adopt a safe harbor
that exempts HIPAA-compliant entities from the entire model act to eliminate the duplicative, administrative burden that this model law would place on them.

This section also establishes the model act as the exclusive standard for data security and the investigation and notification of a data breach. This language indicates that the model act will supersede existing state laws, unless such state laws offer greater protections. We recommend including a provision that would require a state’s existing data security laws to specifically exclude the business of insurance from such laws. By taking this step, licensees will be able to avoid duplicative, and possibly conflicting, data security requirements.

Section 3. Definition, Subsection B. Consumer

The updated definition for “consumer” remains overly broad, potentially subjecting insurers to regulatory scrutiny over matters not involving the insurer-policyholder relationship. As such, the definition should be limited to applicants, insureds, and beneficiaries.

Section 3. Definition, Subsection C. Data Breach

This subsection includes a harm trigger that would limit data breach notification requirements to situations where a licensee is unable to prove with a high degree of certainty that the personally identifiable information released to an unauthorized person has not been used and has been returned or destroyed without further release. While we are happy to see a harm trigger included in this draft, the harm trigger is too broad and would trigger a data breach notification in most instances. We believe that requiring licensees to send notifications on breaches that do not pose the potential for harm will result in hyper-notifications, which may eventually desensitize consumers, commissioners, and other stakeholders to those notices which do inform them of harmful breaches. It would best serve the public’s interest if breach notification requirements are only applied to data breaches that could result in identity theft, fraudulent transactions on financial accounts, and other types of substantial harm.

Section 4, Subsection A. Implementation of an Information Security Program

PIAA is supportive of efforts to recognize that insurers face differing security requirements based on a wide variety of factors. While the third draft expands flexibility beyond the “size and complexity of the licensee,” it fails to factor in the “resources of the insurer” when determining the appropriateness of security measures. We urge you to explicitly expand the scope of flexibility by referencing the “financial resources” of the insurer in this subsection so that insurers are not required to provide security measures that compromise their financial integrity and ability to indemnify their policyholders.

Section 4, Subsection C. Risk Assessment

We are appreciative of the task force’s decision to allow an outside vendor and/or service provider to develop and manage a licensee’s information security program on their behalf.

Section 4, Subsection F. Oversight of Third-Party Service Provider Arrangements

PIAA applauds the elimination of language that would have held licensees liable for the failure of their third-party service providers to protect personal information. While we support the task force’s decision to require that licensees confirm that third-party service providers have the appropriate level of data
security measures in place at the time a contract is signed, it would not be appropriate to require licensees to renegotiate all their third-party service contracts immediately upon the enactment of the new law. Consequently, we recommend that you include a grandfather clause that exempts existing third-party service contracts that are in effect at the time this model law is enacted. Alternatively, you may want to consider giving licensees a minimum of a two-year grace period to update all their third-party service contracts.

**Section 5. Investigation of a Data Breach, Subsection D. Notification to the Commissioner**

This subsection requires a licensee to notify the commissioner that a data breach has occurred within three business days of an ascertained data breach. Furthermore, it requires a licensee to submit as much information as possible from a list of 15 data points. We caution the NAIC against requiring a licensee to submit incomplete information on a data breach solely for the sake of complying with the deadline. Instead, we recommend that you require all “relevant information available” to the licensee within the recommended time frame.

In closing, PIAA appreciates this opportunity to provide input regarding the *Insurance Data Security Act*. We look forward to providing verbal comments to the Cybersecurity Task Force during the upcoming spring national meeting in Denver. Meanwhile, please do not hesitate to contact me should you need any further information.

Sincerely,

Brian K. Atchinson  
President & CEO  
PIAA

CC: Members of the NAIC Cybersecurity Working Group  
Eric Nordman, Director, Regulatory Services and CIPR  
Cody Steinwand, Manager of Security Initiatives