RISK ANALYSIS & CYBERSECURITY GUIDELINES

FOR AGENT USE ONLY

This Risk Analysis recognizes certain activities that fall within the scope of the receipt, transmitting, and storage of non-public-personal information (NPPI). Such activities are subject to various state and federal regulations such as, but not limited to: The **Gramm-Leach-Bliley Act** (**GLB Act** or **GLBA**) is also known as the Financial Modernization **Act** of 1999. It is a United States federal law that requires financial institutions to explain how they share and protect their customers' private information. **HIPAA** (Health Insurance Portability and Accountability Act of 1996) is United States legislation that provides data privacy and security provisions for safeguarding medical information, and (**HITECH**) which is part of the American Recovery and Reinvestment Act (ARRA) of 2009 and creates incentives related to health care information technology, including incentives for the use of electronic health record (EHR) systems among providers. The common goal of most is not all cybersecurity regulations is to secure the privacy of the information received, transmitted, or stored by AIPMA as it is the goal of AIPMA to comply with the intentions of such regulatory requirements.

It is easy to conclude that tamper-proof technical protection mechanisms, such as strong data **anonymization**, a type of information sanitization whose intent is privacy protection. It is the process of either encrypting or removing personally identifiable information from data sets. Therefore, concerning those whose NPPI is not removed, the only option is encryption in order to protect them from data threats. However, it may be such perfect protection for personal information is not, with current technology, achievable. As Charles Darwin noted, "Building a better mousetrap merely results in smarter mice."

The threat environment for AIPMA would include such things as 3rd party vendors, the human error factor, unaddressed changes in technology, breach of data, management responses to a breach of data, insufficient physical protection of data, lack of employee training related to their cybersecurity responsibilities, and inappropriate disposal of data. This list is not exhaustive and is subject to review and change from time to time. Simply stated, there is always going to be potential vulnerability in an information system.

Based upon multiple factors, it is management's conclusion that AIPMA's cybersecurity risk is low. One major factor is that AIPMA does not sell directly to retail customers. Rather, AIPMA is principally a conduit through which information passes. Applications received are sent to the involved insurance carriers. Paramedical exams are done by independent Paramedical companies, and the results are sent to those same insurance companies. PaperClip, Inc. stores Paramedical exam information in electronic format. The overall process is designed to eliminate paper. Additionally, and after hacking into the AIPMA system, one would be faced with the information security in place by PaperClip, as well as the involved insurance carriers.

While there is no absolute guarantee, the uncertainty and potential frequency of threats and their impact can also be reduced by preparation, employee training, and the following of AIPMA's below listed operating principles. Additionally, AIPMA has adopted opportunistic TLS encryption and two-factor authentication.

Principles for Effective Cybersecurity: Due to ever-increasing cybersecurity issues, it has become clear that society has and will continue to adopt regulations to protect non-public personal information in order to provide effective cybersecurity guidance regarding the protection of the insurance sector's data security and infrastructure. The insurance industry looks to state insurance regulators to aid in the identification of uniform standards, to promote accountability across the entire insurance sector, and to provide access to essential information. State insurance regulators look to the insurance industry to join forces in identifying risks and offering practical solutions. The operating principles listed below

are intended to reflect insurance regulatory guidelines that promote the relationships between insurance professionals and consumers.

Principle 1: As employees of AIPMA, we have a responsibility to ensure that any NPPI that is received, stored, and transferred by AIPMA is protected from cybersecurity risks.

Principle 2: Confidential and/or personally identifiable consumer information data that is received, stored, and transferred outside of AIPMA should be appropriately safeguarded.

Principle 3: NPPI includes everything other than age and gender information received, stored, and transmitted to carriers by AIPMA. In the event of a breach, those impacted or potentially impacted should be notified consistent with the various state(s) regulation(s).

Principle 4: In addition to the various state regulations, there are several federal regulations concerning NPPI. Basically, the inappropriate release of NPPI, no matter how it occurs, may be financially significant to AIPMA and must be immediately reported to AIPMA senior management. If you have no proof of any inappropriate breach of NPPI, but your gut feeling is that there might be a problem, you should immediately notify AIPMA senior management.

Principle 5: AIPMA operating guidelines were created as a part of AIPMA's risk analysis. Review of the Risk Analysis, and the operating guidelines, will be reviewed at least annually or more frequently as required by ongoing regulatory changes.

Principle 6: State insurance regulators provide appropriate regulatory oversight, which includes, but is not limited to, conducting risk-based examinations, market conduct examinations, and/or compliance with cybersecurity regulations.

Principle 7: Incident response to insurers, regulators, and consumers is an essential component of an effective cybersecurity program. Such requirements are increasingly becoming part of our agency responsibilities to carriers and regulators.

Principle 8: AIPMA will take appropriate steps to ensure that third-party vendors with which AIPMA has a business relationship have their own NPPI protections in place to such NPPI.

Principle 9: NPPI includes past, present, future plans, physical, mental, behavioral information, descriptive material, social security, driver's license, credit, financial, **or anything other than age and gender.** In the case of the receipt of a subpoena, no response shall be provided without the review and approval of AIPMA's senior management.

Principle 10: A cybersecurity section will be incorporated into AIPMA's Compliance Manuel and become available to all independent agents. Agents requesting cybersecurity information need to seek and rely upon the state insurance regulators in the state(s) in which the business was written and/or seek and rely upon their own legal counsel.

Principle 11: Periodic and timely training of employees is essential. There will be initial training for employees when the Risk Analysis & Cybersecurity Guidelines are introduced and anytime thereafter when deemed necessary, or as otherwise required by regulations.

Principle 12: The NPPI regulations, both state and federal, are complex to the point that many problems can be avoided by simply operating in the spirit of protecting NPPI.

Michigan has enacted the **Insurance Data Security Model Law**. This includes the breach reporting provisions relating to cybersecurity event investigations, regulatory reporting, and individual notifications for breaches that were discovered or subject to notification after December 31, 2019. Other states likely will adopt similar laws; however, not all state laws will have the same provisions. Therefore, reporting and notice requirements will depend on multiple factors.

Disclaimer: *This document is a concept review of a complicated and detailed Michigan law. It is NOT intended and should not in any way be considered legal advice in either Michigan or any other jurisdiction as state laws on the subject of Cybersecurity will frequently not be uniform.*