**Government of Puerto Rico**

**OFFICE OF THE COMMISSIONER OF INSURANCE**

**San Juan, Puerto Rico**

# RULE NO. 108 OF THE REGULATIONS OF THE INSURANCE CODE OF PUERTO RICO

# "CYBERSECURITY STANDARDS FOR THE INSURANCE INDUSTRY"

**Government of Puerto Rico**
**OFFICE OF THE COMMISSIONER OF INSURANCE**
**San Juan, Puerto Rico**

**TABLE OF CONTENTS**

**RULE NO. 108**

**"CYBERSECURITY STANDARDS FOR THE INSURANCE INDUSTRY"**

**TABLE OF CONTENTS**

Government of Puerto Rico
OFFICE OF THE COMMISSIONER OF INSURANCE
San Juan, Puerto Rico

**RULE NO. 108**

**"CYBERSECURITY STANDARDS FOR THE INSURANCE INDUSTRY"**

**SECTION 1. – TITLE**

This Rule shall be known as the "Cybersecurity Standards for the Insurance Industry."

**SECTION 2. – LEGAL AUTHORITY**

This Rule is promulgated pursuant to Section 2.030 of Act No. 77, enacted on June 19, 1957, as amended, the "Insurance Code of Puerto Rico" and Act No. 38-2017, as amended, the "Government of Puerto Rico Uniform Administrative Procedure Act."

**SECTION 3. – PURPOSE**

The purpose of this Rule is to establish cybersecurity standards in the insurance industry and standards for investigating and reporting to the Commissioner a cybersecurity incident related to a Licensee's business, as provided for in this Rule.

**SECTION 4. – EXECUTIVE SUMMARY**

This Rule addresses the growing need to create the necessary safeguards to minimize the risks of unauthorized access to information systems compromising Nonpublic data and information related to the insurance business of a Licensee. Adopting this Rule reflects the commitment of the Office of the Commissioner of Insurance of Puerto Rico to establish a cybersecurity regulatory framework adequate for safeguarding Licensee and consumer-sensitive information collected as part of the underwriting and claims processes in the insurance business, in accordance with the principles of the National Association of Insurance Commissioners (NAIC) established in "Insurance Data Security Law."

To ensure the continuity and relevance of this Rule, the standards of the U.S. National Institute of Standards and Technology (NIST) are used as a guiding principle, whose framework provides the appropriate standards, guidelines, and practices to assist Licensees in managing their cyber risks.

A. To achieve cybersecurity in the insurance industry, this Rule requires Licensees to:

(1) develop, implement, and maintain a Cybersecurity Program;

(2) investigate any cybersecurity events; and

(3) notify the Commissioner of cybersecurity events.

**SECTION 5. – INTERPRETATION**

This Rule may not be construed to create a cause of action for violating its provisions, nor may it be construed to preclude the exercise of any other cause of action that would otherwise exist.

If any conflict arises between the provisions of this Rule, the interpretation that will prevail will be the one that is most favorable for safeguarding the rights of the insured.

**SECTION 6. – APPLICABILITY**

The provisions of this Rule shall apply to any person who holds a license or authorization to transact insurance business, duly issued by the Office of the Commissioner of Insurance of Puerto Rico ("OCI") and who, in turn, uses an Information System, as defined in this Rule.

**SECTION 7. – DEFINITIONS**

For the purposes of this Rule and except where a more specific definition is provided, the following terms shall have the meanings set forth below:

A. "**Multi-Factor Authentication**" means authentication through verification of at least two (2) of the following authentication factors:

(1) Knowledge factors, such as a password; or

(2) Possession factors, such as a token or text message on a mobile phone; or

(3) Inherence factors, such as a biometric characteristic.

B. "**Code**" means the Insurance Code of Puerto Rico, Act No. 77, enacted on June 19, 1957, as amended, 26 L.P.R.A., et seq.

C. "**Commissioner**" means the Commissioner of Insurance of Puerto Rico.

D. "**Consumer**" means any individual, including, but not limited to, applicants, policyholders, insureds, beneficiaries, claimants, and certificate holders who resides in Puerto Rico or who owns insured property in Puerto Rico, and whose Nonpublic Information is in the hands of the Licensee or in the possession, custody, or control of the Licensee.

E. "**Service Contractor**" means a Person, not otherwise defined as a Licensee, that the Licensee contracts to maintain, process, store or otherwise is permitted

access to Nonpublic Information through the services it provides to the Licensee.

F. "**Encryption**" means the transformation of information into a format that results in decreasing the probability of discovering its meaning without using a protective process or key. For the purposes of this Rule, the required encryption must meet the encryption standards established by the U.S. National Institute of Standards and Technology ("NIST").

G. "**State**" means the Government of Puerto Rico.

H. "**Risk Assessment**" means the risk assessment that each Licensee is required to conduct pursuant to Section 8(C) of this Rule.

I. "**Cybersecurity Incident**" means an event that violates Information Systems policies or puts the confidentiality, integrity, or availability of information systems at real or imminent risk. Cybersecurity Incidents do not include events in which the Licensee has determined, using documentary evidence or through a third party qualified in cybersecurity incident response, that the information accessed without authorization has not been used, modified, encrypted, disclosed, or exfiltrated.

J. "**Public Information**" means any information that the Licensee could reasonably believe to be lawfully available to the general public pursuant to federal, state, or local government records, widely distributed media, or disclosures to the public that are required by federal, state, or local law.

For the purposes of this definition, the Licensee shall have a reasonable basis to believe that the information is lawfully disclosed to the general public if the Licensee has taken steps to determine:

(1) That the information is of the type that is available to the general public; and

(2) If a consumer has the power to prevent the information from being made available to the general public and, if so, has not done so.

K. "**Nonpublic Information**" means information that is not available to the public and consists of:

(1) Business-related information of a Licensee, which, if tampered

with or disclosed without authorization or given access to or use thereof, would cause a significant adverse impact to the Licensee's business, operations, or security;

(2) Any information relating to a Consumer, which, because of name, number, mark, or other identifier, could be used to identify the Consumer, in combination with one or more of the following elements:

(a) Social Security number,

(b) Driver's license or alternate identification card for non-drivers,

(c) Account number, credit or debit card number,

(d) Any security code, access code, or password that would allow access to a Consumer's financial account, or

(3) Biometric records. Any information or data about health condition, except age or gender, in any format or medium created by or derived from a health care provider or Consumer and that relates to:

(a) The past, present, or future physical, mental, or behavioral health or condition of a Consumer or a family member of a Consumer;

(b) Health care services provided to a Consumer; or

(c) Payments for a Consumer's health care.

L. "**Person**" means an individual or a non-governmental legal entity including, but not limited to, any non-governmental partnership, corporation, branch, agency, or association.

M. "**Authorized Individual**" means an individual designated and authorized by the Licensee and determined to be necessary and appropriate to have access to the Nonpublic Information held by the Licensee and its information systems in order to carry out their duties.

N. **"Cybersecurity Program"** means the administrative, technical, and physical policies, procedures, and controls used by the Licensee to protect, access, collect, distribute, process, store, use, transmit, dispose of, or otherwise handle data in Information Systems.

O. "**Licensee**" means any natural or legal person who holds a license, authorization, or certificate of authority to transact insurance business in Puerto Rico or is registered or required to be licensed, authorized, or registered pursuant to the Insurance Code of Puerto Rico. This does not include a purchasing group or risk control group that has been established and licensed in another state, or a Licensee acting as a reinsurer and that is domiciled in another state or jurisdiction.

P. "**Information System**" means a defined set of electronic information resources organized to collect, store, reproduce, process, maintain, use, share, disseminate, or dispose of public or nonpublic data, as well as any specialized systems such as industrial and process control systems, telephone switching systems, private branch exchange (PBX) systems, and environmental control systems.

**SECTION 8. – CYBERSECURITY PROGRAM**

A. Implementation of a Cybersecurity Program:

Depending on the size and complexity of the Licensee, the nature and scope of the Licensee's activities, including the use of Service Contractors, and the sensitivity of the Nonpublic Information used by the Licensee or in the Licensee's possession, custody, or control, each Licensee shall develop, implement, maintain, and document a comprehensive written digital information security program, based on the risk assessment of the Licensee and containing the administrative, technical, and physical safeguards for the protection of the Nonpublic Information and the information system of the Licensee.

B. Objectives of the Cybersecurity Program:

The Licensee shall design the Cybersecurity Program to:

(1) Protect and ensure the confidentiality, integrity, and availability of the Nonpublic Information stored in the Information Systems, and ensure the security of the Information System;

(2) Protect against unauthorized access to or use of Nonpublic Information, and minimize the possibility of harm to any Consumer; and

(3) Define and periodically reevaluate the retention period of Nonpublic Information and the mechanism for destroying it when it is no longer

needed.

C. The Licensee shall conduct a Risk Assessment to:

(1) Designate one or more employees, affiliates, third-party vendors, or Service Contractors designated to act on behalf of the Licensee to be responsible for the Cybersecurity Program;

(2) Identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, alteration, destruction, or use of Nonpublic Information, including the security of Information Systems and Nonpublic Information that are accessible to, or in the possession of, Service Contractors;

(3) Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Nonpublic Information;

(4) Design and assess the sufficiency of the policies, procedures, Information Systems, and other safeguards established to manage these threats, including consideration of threats in each relevant area of the Licensee's operations, such as:

(a) Employee training and management;

(b) Information systems, including network and software design, as well as data classification, governance, processing, electronic storage, transmission, and disposition; and

(c) Detecting, preventing, and responding to attacks, intrusions, or other system failures.

(5) Implement information safeguards to manage threats identified in its ongoing assessment, and at least annually, assess the effectiveness of key controls, systems, and procedures of the safeguards.

(6) If artificial intelligence (AI) algorithms, programs, or technology have been adopted, the corresponding policies and processes shall be assessed in order to:

(a) Ensure that data used by AI is accessed and processed securely, particularly protecting Nonpublic Information, including unauthorized access to predictive models as needed;

(b) Fulfill the Licensee's privacy and security policies, as well as the compliance requirements of any agency, corporation, or government instrumentality, regulatory agency, or other oversight entity under any state or federal law; and

(c) Measure AI performance on a regular basis to validate proper performance in relation to data confidentiality, integrity, and availability, as applicable.

D. Risk Management:

Based on its risk assessment, the Licensee shall:

(1) Design its Cybersecurity Program to mitigate the identified risks, based on the size and complexity of the Licensee's activities, including the use of Service Contractors and the sensitivity of the Nonpublic Information used by or in the possession, custody, or control of the Licensee.

(2) Implement the following security measures, as warranted by the Licensee's infrastructure, staff, operation, and information systems:

(a) Maintain a formal training program on cyber risk modalities for the staff and keep track of employee performance in the program.

(b) Provide employees with Cybersecurity Program training and assign them responsibilities within the program;

(c) Establish effective access controls on Information Systems, including controls to authenticate (such as multi-factor authentication) and allow access only to authorized individuals to protect against the unauthorized acquisition, alteration, disclosure, or destruction of Nonpublic Information;

(d) Maintain an oversight program for service providers with access to Nonpublic Information, which includes service agreements and requires cybersecurity controls;

(e) Identify and manage the information, personnel, devices, systems, and facilities that enable the Licensee to achieve its

business purposes in accordance with their relative importance to the business objectives and risk management strategy of the organization;

(f) Restrict physical access to areas where Nonpublic Information is located so that it is only accessible to authorized individuals;

(g) Protect, by encryption or other appropriate means, all Nonpublic Information while being transmitted over an external network and all Nonpublic Information stored on a laptop computer or other portable computing or electronic storage device or medium;

(h) Adopt secure development practices for all applications that are developed in-house for the use of the Licensee and procedures for evaluating, assessing, or testing the security of applications developed by external resources used by the Licensee;

(i) Modify the Information System in accordance with the Licensee's Cybersecurity Program;

(j) Regularly test and monitor systems and procedures to detect actual and attempted attacks on or intrusions into the Information System and the network, as well as document the outcome of these tests;

(k) Include backup, safekeeping, and management processes ("audit logs") within the Cybersecurity Program designed to detect and respond to Cybersecurity Incidents and to reconstruct material financial transactions in order to provide adequate support to the normal operations and obligations of the Licensee;

(l) Implement measures to protect against the destruction, loss, or damage of Nonpublic Information due to environmental hazards, such as fire and water damage or other catastrophes or technological failures; and

(m) Develop, implement, and maintain procedures for the secure disposal of Nonpublic Information in any format.

(3) Include cybersecurity risks in the Licensee's business risk management process and in the reports required in Sections 32.040 and 53.070 of the Insurance Code of Puerto Rico and Rule 104 on Corporate Governance.

(4) Stay informed regarding new threats or vulnerabilities and use reasonable security measures when sharing information relative to the manner of sharing and the type of information shared.

(5) Perform regular vulnerability tests on their Information Systems with tools that clearly identify vulnerabilities, as indicated by this Office.

E. Oversight by the Board of Directors:

If the Licensee has a Board of Directors, the Board or an appropriate committee of the Board shall, at a minimum:

(1) Require the Licensee's executive management or the person delegated by the management to develop, implement, and maintain the Cybersecurity Program of the Licensee.

(2) Require the executive management of the Licensee or the person delegated by the management of the Licensee to submit at least once (1) a year a report, for the approval and signature of the Board of Directors, on the following information:

(a) The overall condition of the Cybersecurity Program and the Licensee's compliance with this Rule; and

(b) Relevant or material matters related to the Cybersecurity Program that address risk assessment, risk management, and control decisions, relationships with Service Contractors, the results of tests performed, Cybersecurity Incidents or violations, and management's response thereto, and recommendations for changes to be made to the Cybersecurity Program.

(3) If the executive management of the Licensee delegates any of its responsibilities pursuant to Section 8 of this Rule, it shall oversee the development, implementation, and maintenance of the Licensee's Cybersecurity Program prepared by the delegate and shall receive a report from the delegate that complies with the requirements of the report to the Board of Directors indicated above.

F. Oversight of Relationships with Service Contractors:

(1) The Licensee shall perform due diligence in selecting the Service Contractor, and

(2) The Licensee shall require by contract or service agreement that the Service Contractor implement appropriate administrative, technical, and physical measures to protect and secure the Information Systems and Nonpublic Information that are accessible to or in the possession of the Service Contractor.

G. Program Adjustments:

The Licensee shall monitor, evaluate, and adjust, as indicated, the Cybersecurity Program in accordance with any relevant changes in technology, the sensitivity of Nonpublic Information, internal or external threats to information, and changes in the Licensee's business relationships, such as mergers and acquisitions, alliances, and joint ventures, outsourcing arrangements and changes to Information Systems.

H. Incident Response Plan:

(1) As part of its Cybersecurity Program, each Licensee shall establish a written incident response plan that provides for a prompt response and recovery in the event of a Cybersecurity Incident that compromises the confidentiality, integrity, or availability of the Nonpublic Information in its possession, the Licensee's Information Systems, or the continuing functionality of any aspect of the Licensee's business or operations.

(2) The incident response plan shall address the following:

(a) The internal process for responding to a Cybersecurity Incident;

(b) The objectives of the incident response plan;

(c) A clear definition of the roles, responsibilities, and levels of decision-making authority, including names of employees and incident response providers;

(d) External and internal communications and the manner in which information is shared;

(e) Identification of requirements for the remediation of any identified weaknesses in the Information Systems and associated controls;

(f) Documentation and preparation of reports regarding Cybersecurity Incidents and related response activities; and

(g) The evaluation and revision of the incident response plan, as necessary after a Cybersecurity Incident.

I. Annual Certification to the Commissioner

No later than June 30 of each year, all Licensees domiciled in Puerto Rico shall submit to the Commissioner a written statement certifying that they are in compliance with the requirements set forth in Section 8 of this Rule.

All Licensees shall maintain for inspection by the Commissioner, all records, forms, and data on which such certification is based for a period of five (5) years. Licensees must conduct the self-assessment of their external vulnerability tests on a biannual basis. To the extent that the Licensee has identified areas, systems, or processes that require material improvement, updating, or redesign, the Licensee shall document the identification and remedial efforts planned and implemented to address such areas, systems, or processes. Such documentation shall be available to the Commissioner for inspection at any time.

**SECTION 9. – INVESTIGATION OF A CYBERSECURITY INCIDENT**

A. If the Licensee learns that a Cybersecurity Incident has occurred or may have occurred, the Licensee or the outside vendor and/or Service Contractor designated to act on behalf of the Licensee shall conduct an investigation as soon as possible and prepare a written report thereof.

B. During the investigation, the Licensee or the outside vendor and/or Service Contractor designated to act on behalf of the Licensee shall, at a minimum:

(1) Determine whether a Cybersecurity Incident has occurred;

(2) Assess the nature and scope of the Cybersecurity Incident;

(3) Identify any Nonpublic Information that may have been affected in the Cybersecurity Incident; and

(4) Perform or oversee reasonable measures to restore the security of the Information Systems affected by the Cybersecurity Incident to prevent further acquisition, disclosure, or use of Nonpublic Information in the possession, custody, or control of the Licensee.

C. If the Licensee learns that a Cybersecurity Incident has occurred or may have occurred in a system maintained by a Service Contractor, the Licensee shall complete the steps listed in subsection B or confirm and document that the Service Contractor has completed such steps.

D. The Licensee shall maintain records of all Cybersecurity Incidents for at least five (5) years from the date of the incident and shall submit such records upon demand of the Commissioner.

**SECTION 10. – NOTIFICATION OF A CYBERSECURITY INCIDENT**

A. Notification to the Commissioner

The Licensee shall notify the Commissioner of a Cybersecurity Incident as promptly as possible, within 72 hours after the time it has been determined that a Cybersecurity Incident has occurred when any of the following criteria are met:

(1) The Licensee reasonably believes that the Nonpublic Information involved in the Cybersecurity Incident impacts 250 or more Consumers residing in Puerto Rico, and that the Cybersecurity Incident:

(a) Impacts the Licensee in a manner that requires notice to any government agency, corporation or instrumentality, regulatory agency, or other supervisory entity pursuant to any state or federal law, or

(b) Has a reasonable probability of causing material harm to:

i. Consumers residing in Puerto Rico, or

ii. Any material aspect of the normal operations of the Licensee.

B. The Licensee shall provide as much of the information set forth below as possible in electronic format as directed by the Commissioner. The Licensee shall have the obligation to update and supplement initial and subsequent notifications to the Commissioner related to the Cybersecurity Incident.

(1) Date of the Cybersecurity Incident;

(2) Description of how the information was disclosed, lost, or stolen, or how the security breach to access it was conducted, including the specific roles and responsibilities of Service Contractors, if any;

(3) How the Cybersecurity Incident was discovered;

(4) Whether any lost, stolen, or breached information has been recovered and, if so, how this was done;

(5) The identity of the source of the Cybersecurity Incident;

(6) Whether the Licensee filed a complaint with the police or has notified any regulatory, government, or law enforcement agency, and if so, when the notice was filed;

(7) Description of the specific types of data acquired without authorization. Specific types of data, e.g., medical information, financial information, or information that allows the Consumer to be identified;

(8) The period during which the Information System was compromised by the Cybersecurity Incident;

(9) The total number of consumers in Puerto Rico affected, or that could be affected, by the Cybersecurity Incident. The Licensee shall provide the best estimate in the initial report to the Commissioner and shall update the estimate in each subsequent report to the Commissioner in accordance with this Section;

(10) The results of any internal inquiry that identified a failure in automated controls or internal procedures, or that confirmed that all automated controls and internal procedures were complied with;

(11) Description of efforts being undertaken to remediate the situation that allowed the Cybersecurity Incident to occur;

(12) A copy of the Licensee's privacy policy and a statement outlining the steps the Licensee will take to investigate and notify Consumers affected by the Cybersecurity Incident; and

(13) The name of a contact person who has knowledge of the Cybersecurity Incident and is authorized to act on behalf of the Licensee.

C. Notification to Consumers.

The Licensee shall comply with the Citizen Information on Data Banks Security Act, Act No. 111-2005, as amended, as applicable, and shall provide the Commissioner with a copy of the notice sent to Consumers, as provided by law, when the Licensee is required to notify the Commissioner pursuant to subsection A of this section. Notification under Act No. 111-2005 shall be made if the personal or non-personal information is protected with cryptographic keys, other than a password.

D. Notice Regarding Cybersecurity Incidents of Service Contractors:

(1) If the Licensee becomes aware of a Cybersecurity Incident in a system maintained by a Service Contractor, the Licensee shall treat such incident as provided in subsection A of this section.

(2) The deadline for notification by the Licensee shall be calculated from the day after the Service Contractor notifies the Licensee of the Cybersecurity Incident or the Licensee becomes aware of the Cybersecurity Incident, whichever occurs first.

(3) Nothing in this Rule shall prevent or impair agreements between a Licensee and another, between a Licensee and a Service Contractor, or a Licensee with any other person to conduct the investigation set forth in Section 9 of this Rule or to fulfill the notice requirements set forth in this Section.

E. Notice Regarding Cybersecurity Incidents of Reinsurers to Insurers:

(1) (a) In the event of a Cybersecurity Incident involving Nonpublic Information that is used by a Licensee acting as a reinsurer or that is in

the possession, custody, or control of a Licensee acting as a reinsurer and that does not have a direct contractual relationship with the affected Consumers, the reinsurer shall notify the affected ceding insurers and the Commissioner of its state of domicile within 72 hours of determining that a Cybersecurity Incident has occurred.

(b) Ceding insurers that have a direct contractual relationship with affected Consumers shall fulfill the Consumer notification requirements set forth in subsection (C) of this section and any other requirements relating to Cybersecurity Incidents set forth in this section.

(2) (a) In the event of a Cybersecurity Incident involving information in the possession, custody, or control of a Service Contractor of a Licensee that is a reinsurer, the reinsurer shall notify the affected ceding insurers and the Commissioner of their state of domicile within 72 hours of receiving notification from their Service Contractor that a Cybersecurity Incident has occurred.

(b) Ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements set forth in subsection (C) of this section and any other notification requirements relating to the Cybersecurity Incidents set forth in this section.

F. Notice Regarding Cybersecurity Incidents of Insurers or Health Service Organizations to Producers:

In the event of a Cybersecurity Incident involving information that is in the possession, custody, or control of a Licensee that is an insurer or its Service Contractor and that the insurer's services were provided to the Consumer through an insurance producer or intermediary, the insurer or health service organization shall notify the producer or intermediary of record of all affected consumers as soon as possible.

The insurer or health service organization is excused from this obligation for those instances in which it does not have current information about the insurance producer or intermediary for any given Consumer.

**SECTION 11. – POWER OF THE COMMISSIONER**

A. The Commissioner shall have the power to examine and investigate Licensees to determine whether any Licensee has acted or is currently acting in violation of this Rule. This power is in addition to the Commissioner's power to investigate and conduct examinations as provided in the Insurance Code of Puerto Rico, particularly Chapter 2 of the Insurance Code of Puerto Rico. Such investigation or examination shall be conducted pursuant to the provisions of Section 2.030(12) of the Insurance Code. If it is necessary to retain outside technical staff to perform the expert investigation or audit, the Insurance Commissioner may request reimbursement of the expenses incurred, provided that a detailed account of such expenses is submitted. In accordance with the provisions of Section 2.130 of the Insurance Code of Puerto Rico, the Licensee must make accessible to the Commissioner its Digital Data Security or Cybersecurity Program and all documents in the Licensee's possession related to the required or collected protocols and information relating to this Rule.

B. Whenever the Commissioner has reason to believe that a Licensee has acted or is acting in violation of this Rule, the Commissioner may take the necessary actions to enforce the provisions of this Rule, which includes the imposition of penalties as provided for in this Rule and the Insurance Code of Puerto Rico.

**SECTION 12. –CONFIDENTIALITY**

A. Any document, material, or other information in the control or possession of the Office of the Commissioner of Insurance provided by a Licensee or employee or agent acting on behalf of the Licensee pursuant to Section 8(I) and Section 10(B)(2), (3), (4), (5), (8), (10), and (11) of this Rule or that are obtained by the Commissioner in the course of an investigation or examination pursuant to Sections 8 and 10 of this Rule shall be confidential by law and privileged, shall not be subject to disclosure to the public pursuant to Section 2.090 of the Insurance Code, nor to disclosure by subpoena or court order, and shall not be subject to discovery or admissible as evidence in any private action. However, the Commissioner is authorized to use the documents, materials, or other information in any regulatory or legal action brought by the Commissioner in the performance of their duties.

B. Neither the Commissioner nor any person who received documents, materials, or other information while acting under the authority of the Commissioner shall be permitted or required to testify in a private action concerning any confidential documents, materials, or information subject to subsection A.

C. In the performance of the Commissioner's duties, under this Rule, the Commissioner may:

(1) Share documents, materials, or other information, including confidential or privileged documents, materials, or information subject to subsection A, with other state, federal, and international regulatory agencies, with the National Association of Insurance Commissioners, its affiliates, or subsidiaries, and with state, federal, and international law enforcement authorities, provided that the recipient of such documents, materials or information agrees in writing to maintain the confidentiality and privileged status thereof;

(2) Receive documents, materials, or information, including documents, materials, or information that would otherwise be confidential and privileged, from the National Association of Insurance Commissioners, its affiliates, or subsidiaries, and from law enforcement and regulatory officials of domestic or foreign jurisdictions, and shall maintain as confidential or privileged any document, material, or information received with notice or the understanding that it is confidential or privileged under the laws of the jurisdiction that is the source of the document, material, or information;

(3) Share documents, materials, or other information, subject to the provisions of subsection A of this section, with a third-party consultant or vendor, provided that the consultant agrees in writing to maintain the confidentiality and privileged status of the document, material, or other information; and

(4) Enter into agreements to share and use information consistent with this subsection C.

D. Disclosure to the Commissioner under this section or as a result of sharing the documents, materials, or information as authorized in subsection C shall not result in the waiver of the applicable confidentiality or privileged status.

E. Nothing in this Rule shall prohibit the Commissioner from disclosing the final results of adjudicated matters that are subject to public inspection, as provided in Section 2.090 of the Insurance Code of Puerto Rico, to a database or other clearinghouse service maintained by the National Association of Insurance Commissioner (NAIC), its affiliates or subsidiaries.

**SECTION 13. –EXCEPTIONS**

A. The provisions of this Rule shall not apply in the following circumstances:

(1) A Licensee with fifteen (15) or fewer employees shall be exempt from Section 8 of this Rule;

(2) An employee, agent, representative, or designee of a Licensee, who is also a Licensee, is exempt from Section 8 and need not develop its own Cybersecurity Program to the extent that the employee, agent, representative, or designee is covered by the Cybersecurity Program of the other Licensee;

(3) A Licensee that has established and maintains a Cybersecurity Program pursuant to the requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the HIPAA Security Rule (45 C.F.R. Part 160 and Subpart A and C of Part 164) shall be considered to meet the requirements of Section 8 of this Rule, provided the Licensee submits a written certification of compliance;

(4) A Licensee that is also an affiliate or subsidiary of a financial institution, as defined in Act No. 4-1985, as amended, and maintains a Cybersecurity Program in accordance with interagency guidelines that establish standards for protecting customer information, as set forth in section 501 of the Gramm-Leach-Bliley Act (15 U.S.C. 6801) shall be considered to meet the requirements of Section 8 of this Rule, provided the Licensee submits a written certification of compliance.

B. In the case that a Licensee ceases to qualify for an exception, such Licensee shall have 180 days to comply with this Rule.

**SECTION 14.** – **PENALTIES**

If a Licensee violates this Rule, the Commissioner may impose a penalty of up to $10,000 per violation as authorized by Section 2.250 of the Insurance Code of Puerto Rico.

**SECTION 15. – SEVERABILITY**

If any section, part, or paragraph of this Rule is found to be unconstitutional, null, or void by a court of competent jurisdiction, such determination shall not affect the validity of the remaining provisions of this Rule.

**SECTION 16. –EFFECTIVE DATE**

The provisions of this Rule shall take effect thirty (30) days after their filing with the Department of State of Puerto Rico, in accordance with the provisions of Act No. 38-2017, supra. Licensees shall have a period of six (6) months to implement the provisions of this Rule.

_____

**ALEXANDER S. ADAMS-VEGA, ESQ.**

**COMMISSIONER OF INSURANCE OF PUERTO RICO**

Date of Approval: September 9, 2024

Date of Filing with the Department of State:

Date of Filing with the Library of the Legislature: