Amendment No. 320

Senate Amendment to Senate Bill No. 21 (BDR 57-221)

Proposed by: Senate Committee on Commerce and Labor

Amends: Summary: No Title: No Preamble: No Joint Sponsorship: No Digest: Yes

ASSEMBLY ACTION		Initial and Date	SENATE ACTION		Initial and Date
Adopted ☐	Lost ☐		Adopted ☐	Lost ☐	
Concurred In ☐	Not ☐		Concurred In ☐	Not ☐	
Receded ☐	Not ☐		Receded ☐	Not ☐	

EXPLANATION: Matter in (1) ***blue bold italics*** is new language in the original bill; (2) variations of **green bold underlining** is language proposed to be added in this amendment; (3) ~~red strikethrough~~ is deleted language in the original bill; (4) ~~purple double strikethrough~~ is language proposed to be deleted in this amendment; (5) orange double underlining is deleted language in the original bill proposed to be retained in this amendment.

SENATE BILL NO. 21–COMMITTEE ON COMMERCE AND LABOR

(ON BEHALF OF THE DIVISION OF INSURANCE OF THE DEPARTMENT OF BUSINESS AND INDUSTRY)

PREFILED NOVEMBER 15, 2018

Referred to Committee on Commerce and Labor

SUMMARY—Enacts the Insurance Data Security Law. (BDR 57-221)

FISCAL NOTE: Effect on Local Government: No.
Effect on the State: Yes.

~

EXPLANATION – Matter in ***bolded italics*** is new; matter between brackets [~~omitted material~~] is material to be omitted.

AN ACT relating to cybersecurity; enacting the Insurance Data Security Law; requiring certain licensees with licenses or other authorizations related to the provision and administration of insurance to develop, implement and maintain an information security program that meets certain requirements; establishing requirements for the selection and oversight of third-party service providers by such licensees; requiring certain insurers to submit to the Commissioner of Insurance an annual statement certifying their compliance with certain cybersecurity requirements; enacting provisions governing the response of certain licensees to a cybersecurity event; authorizing the Commissioner to investigate and take disciplinary action against licensees for violations of certain cybersecurity requirements; making certain information obtained by the Commissioner confidential and privileged; providing penalties; and providing other matters properly relating thereto.

Legislative Counsel's Digest:

This bill adds new provisions to the Nevada Insurance Code in conformance with the National Association of Insurance Commissioners' Insurance Data Security Model Law.

Section 19 of this bill requires a licensee, not later than January 1, 2021, to develop and implement a comprehensive written information security program containing administrative, technical and physical safeguards for the protection of nonpublic information and the licensee's information systems, which the licensee is required to monitor, evaluate and adjust as appropriate. **Section 19** also requires a licensee to assess the risks within its organization, implement certain security measures based on those risks and create an incident response plan to direct the response to and recovery from a cybersecurity event. **Section 19** also provides that, beginning on January 1, 2022, a licensee is required to exercise diligence in selecting a third-party service provider and to require any such third-party service provider to implement appropriate measures to protect and secure its information systems and any nonpublic information held by the third-party security provider. Finally, **section 19** provides that, not later than February 15, 2021, and annually thereafter, each insurer domiciled in this State is

required to submit to the Commissioner of Insurance a statement certifying that the insurer is in compliance with the requirements established by **section 19**.

Section 24 of this bill provides that certain insurers are exempt from the requirements imposed by **section 19**.

Section 20 of this bill requires a licensee to conduct an investigation if a cybersecurity event occurs or may have occurred and specifies the minimum requirements for such an investigation. If a licensee learns that a cybersecurity event occurred or may have occurred in a system maintained by a third-party service provider, the licensee is required to investigate the cybersecurity event or confirm and document that the third-party service provider has completed such an investigation.

Section 21 of this bill requires certain licensees to notify the Commissioner of any cybersecurity event and to notify consumers of the cybersecurity event in accordance with existing law. **Section 21** also requires an assuming insurer to notify its affected ceding insurer and an insurer who was contacted by a consumer through an independent insurance producer to notify the producer of record for that consumer, if the producer of record is known. Under **section 21**, the ceding insurer or independent insurance producer is required to notify consumers of the cybersecurity event in accordance with existing law.

Section 22 of this bill authorizes the Commissioner to examine and investigate a licensee for violations of the requirements established by this bill and to take action to enforce those provisions.

Sections 23 and 26 of this bill establish that certain information which is obtained by the Commissioner **, or obtained from the Commissioner by the National Association of Insurance Commissioners or a third-party consultant or vendor,** in relation to cybersecurity is confidential and privileged, except for certain limited purposes.

Section 25 of this bill authorizes the Commissioner to suspend or revoke a license, certificate of authority or registration issued pursuant to the Nevada Insurance Code, to impose an administrative fine and to adopt regulations. **Section 25** also authorizes a licensee to request a hearing on any administrative action taken by the Commissioner.

THE PEOPLE OF THE STATE OF NEVADA, REPRESENTED IN SENATE AND ASSEMBLY, DO ENACT AS FOLLOWS:

Section 1. Title 57 of NRS is hereby amended by adding thereto a new chapter to consist of the provisions set forth as sections 2 to 25, inclusive, of this act.

Sec. 2. ***This chapter may be cited as the Insurance Data Security Law.***

Sec. 3. ***1. The purpose and intent of this chapter is to establish standards for data security and standards for the investigation of and notification to the Commissioner of a cybersecurity event applicable to licensees.***

2. This chapter may not be construed to create or imply a private cause of action for violation of its provisions nor may it be construed to curtail a private cause of action which would otherwise exist in the absence of this chapter.

Sec. 4. ***As used in this chapter, unless the context otherwise requires, the words and terms defined in sections 5 to 18, inclusive, of this act have the meanings ascribed to them in those sections.***

Sec. 5. ***"Authorized individual" means an individual known to and screened by the licensee and determined to be necessary and appropriate to have access to the nonpublic information held by the licensee and its information system.***

Sec. 6. ***"Consumer" means an individual, including, without limitation, an applicant, policyholder, insured, beneficiary, claimant or certificate holder, who is a resident of this State and whose nonpublic information is in the possession, custody or control of a licensee.***

Sec. 7. *1. "Cybersecurity event" means an event resulting in unauthorized access to or disruption or misuse of an information system or nonpublic information stored on such an information system.*

2. The term does not include:

(a) The unauthorized acquisition of encrypted nonpublic information if the encryption, process or key is not also acquired, released or used without authorization; or

(b) An event with regard to which the licensee has determined that the nonpublic information accessed by an unauthorized person has not been used or released and has been returned or destroyed.

Sec. 8. *"Encrypted" means the transformation of data into a form which results in a low probability of assigning meaning without the use of a protective process or key.*

Sec. 9. *"Information security program" means the administrative, technical and physical safeguards that a licensee uses to access, collect, distribute, process, protect, store, use, transmit, dispose of or otherwise handle nonpublic information.*

Sec. 10. *"Information system" means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of electronic nonpublic information, as well as any specialized system such as industrial or process controls systems, telephone switching and private branch exchange systems and environmental control systems.*

Sec. 11. *"Licensee" means any person licensed, authorized to operate or registered, or required to be licensed, authorized or registered, pursuant to this title. The term does not include ~~(a)~~ :*

1. Individual employees of insurers or agencies that are not owners, partners, officers or members of the insurer or agency;

2. An employer who possesses a certification as a self-insured employer pursuant to NRS 616B.312;

3. A purchasing group or a risk retention group chartered and licensed in a state other than this State ; or ~~(a licensee)~~

4. A person that is acting as an assuming insurer that is domiciled in another state or jurisdiction.

Sec. 12. *"Multifactor authentication" means authentication through verification of at least two of the following types of authentication factors:*

1. Knowledge factors, such as a password;

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

3. Inherence factors, such as biometric characteristics.

Sec. 13. *"Nonpublic information" means electronic information that is not publicly available information and is:*

1. Business-related information of a licensee the tampering with which, or unauthorized disclosure, access or use of which, would cause a material adverse impact to the business, operations or security of the licensee.

2. Any information concerning a consumer which because of name, number, personal mark or other identifier can be used to identify such consumer, in combination with any one or more of the following data elements:

(a) Social security number;

(b) Driver's license number or non-driver identification card number;

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

(d) Any security code, access code or password that would permit access to a consumer's financial account; or

(e) Biometric records.

3. Any information or data, except age or gender, in any form or medium created by or derived from a health care provider or a consumer that can be used to identify a particular consumer and that relates to:

(a) The past, present or future physical, mental or behavioral health or condition of any consumer or a member of the consumer's family;

(b) The provision of health care to any consumer; or

(c) Payment for the provision of health care to any consumer.

Sec. 14. *"Person" means any individual or any nongovernmental entity, including, without limitation, any nongovernmental partnership, corporation, branch, agency or association.*

Sec. 15. *1. "Publicly available information" means any information that a licensee has a reasonable basis to believe is lawfully made available to the general public from:*

(a) Federal, state or local governmental records;

(b) Widely distributed media; or

(c) Disclosures to the general public that are required to be made by federal, state or local law.

2. For the purposes of this section, a licensee has a reasonable basis to believe that information is lawfully made available to the general public if the licensee has taken steps to determine:

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

(b) Whether a consumer can direct that the information not be made available to the general public and, if so, that such consumer has not done so.

Sec. 16. *"Risk assessment" means the risk assessment that each licensee is required to conduct under section 19 of this act.*

Sec. 17. *"State" means the State of Nevada.*

Sec. 18. *"Third-party service provider" means a person, other than a licensee, that contracts with a licensee to maintain, process or store or otherwise is permitted access to nonpublic information through the person's provision of services to the licensee.*

Sec. 19. *1. Commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities, including any use of third-party service providers, and the sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody or control, each licensee shall, not later than January 1, 2021, develop, implement and maintain a comprehensive, written information security program based on the licensee's risk assessment and that contains administrative, technical and physical safeguards for the protection of nonpublic information and the licensee's information system.*

2. A licensee's information security program must be designed to:

(a) Protect the security and confidentiality of nonpublic information and the security of the information system;

(b) Protect against threats or hazards to the security or integrity of nonpublic information and the information system;

(c) Protect against unauthorized access to or use of nonpublic information and minimize the likelihood of harm to any consumer; and

(d) Define and periodically reevaluate a schedule for retention of nonpublic information and a mechanism for its destruction when no longer needed.

3. To assess risk within its organization, a licensee shall, not later than January 1, 2021:

(a) Designate one or more employees, an affiliate or an outside vendor designated to act on behalf of the licensee who is responsible for the information security program;

(b) Identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration or destruction of nonpublic information, including the security of information systems and nonpublic information that are accessible to, or held by, third-party service providers;

(c) Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the nonpublic information;

(d) Assess the sufficiency of policies, procedures, information systems and other safeguards in place to manage these threats, including consideration of threats in each relevant area of the licensee's operations, including, without limitation:

(1) Employee training and management;

(2) Information systems, including, without limitation, network and software design, as well as information classification, governance, processing, storage, transmission and disposal; and

(3) Detecting, preventing and responding to attacks, intrusions or other system failures; and

(e) Implement information safeguards to manage the threats identified in its ongoing assessment and, not less than annually, assess the effectiveness of the safeguards' key controls, systems and procedures.

4. Based on its risk assessment, the licensee shall, not later than January 1, 2021:

(a) Design its information security program to mitigate the identified risks, commensurate with the size and complexity of the licensee and the nature and scope of the licensee's activities, including, without limitation, its use of third-party service providers, and the sensitivity of the nonpublic information used by the licensee or in the licensee's possession, custody or control;

(b) Determine which security measures listed below are appropriate and implement such security measures:

(1) Place access controls on information systems, including, without limitation, controls to authenticate and permit access only to authorized individuals to protect against the unauthorized acquisition of nonpublic information;

(2) Identify and manage the data, personnel, devices, systems and facilities that enable the organization to achieve business purposes in accordance with their relative importance to business objectives and the organization's risk strategy;

(3) Restrict physical access to ~~[physical locations containing]~~ nonpublic information ~~[only]~~ to authorized individuals ~~[.]~~ only;

(4) 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 storage device or media;

(5) Adopt secure development practices for in-house developed applications utilized by the licensee and procedures for evaluating, assessing or testing the security of externally developed applications utilized by the licensee;

(6) Modify the information system in accordance with the licensee's information security program;

(7) Utilize effective controls, which may include, without limitation, multi-factor authentication procedures for any individual accessing nonpublic information;

(8) Regularly test and monitor systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems;

(9) Include audit trails within the information security program designed to detect and respond to cybersecurity events and designed to reconstruct material financial transactions sufficient to support normal operations and obligations of the licensee;

(10) Implement measures to protect against destruction, loss or damage of nonpublic information due to environmental hazards, such as fire and water damage or other catastrophes or technological failures; and

(11) Develop, implement and maintain procedures for the secure disposal of nonpublic information in any format;

(c) Include cybersecurity risks in the licensee's enterprise risk management process;

(d) Stay informed regarding emerging threats or vulnerabilities and utilize reasonable security measures when sharing information relative to the character of the sharing and the type of information shared; and

(e) Provide its personnel with cybersecurity awareness training that is updated as necessary to reflect risks identified by the licensee in the risk assessment.

5. If the licensee has a board of directors, the board or an appropriate committee of the board shall, at a minimum:

(a) Require the licensee's executive management or its delegates to develop, implement and maintain the licensee's information security program in accordance with this section; and

(b) After the licensee has developed and implemented its information security program, require the licensee's executive management or its delegates to report in writing, at least annually, the following information:

(1) The overall status of the information security program and the licensee's compliance with this chapter; and

(2) Material matters related to the information security program, addressing issues such as risk assessment, risk management and control decisions, third-party service provider arrangements, the results of testing, cybersecurity events or violations and management's responses thereto and recommendations for changes in the information security program.

6. If executive management delegates any of its responsibilities under this section, it shall oversee the development, implementation and maintenance of the licensee's information security program prepared by the delegates and shall receive a report from the delegates complying with the requirements of the report to the board of directors pursuant to paragraph (b) of subsection 5.

7. Beginning on January 1, 2022, a licensee shall oversee all third-party service provider arrangements, including, without limitation, by:

(a) Exercising due diligence in selecting its third-party service provider; and

(b) Requiring a third-party service provider to implement appropriate administrative, technical and physical measures to protect and secure the information systems and nonpublic information that are accessible to, or held by, the third-party service provider.

8. After a licensee has implemented an information security program, the licensee shall monitor, evaluate and adjust, as appropriate, the information security program consistent with any relevant changes in technology, the sensitivity of its nonpublic information, internal or external threats to

information and the licensee's own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to information systems.

9. As part of its information security program, each licensee shall, not later than January 1, 2021, establish a written incident response plan designed to promptly respond to, and recover from, any cybersecurity event that compromises the confidentiality, integrity or availability of nonpublic information in its possession, the licensee's information systems or the continuing functionality of any aspect of the licensee's business and operations. Such incident response plan must address the following areas:

(a) The internal process for responding to a cybersecurity event;

(b) The goals of the incident response plan;

(c) The definition of clear roles, responsibilities and levels of decision-making authority;

(d) External and internal communications and information sharing;

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

(f) Documentation and reporting regarding cybersecurity events and related incident response activities; and

(g) The evaluation and revision as necessary of the incident response plan following a cybersecurity event.

10. Not later than February 15, 2021, and not later than February 15 of each year thereafter, each insurer domiciled in this State shall submit to the Commissioner a written statement certifying that the insurer is in compliance with the requirements set forth in this section. Each insurer shall maintain for examination by the Division all records, schedules and data supporting this certification for a period of 5 years. To the extent an insurer has identified areas, systems or processes that require material improvement, updating or redesign, the insurer shall document the identification and the remedial efforts planned and underway to address such areas, systems or processes. Such documentation must be available for inspection by the Commissioner.

Sec. 20. *1. If the licensee learns that a cybersecurity event has or may have occurred, the licensee or an outside vendor or service provider designated to act on behalf of the licensee shall conduct a prompt investigation.*

2. During the investigation, the licensee or the outside vendor or security provider designated to act on behalf of the licensee shall, at a minimum, determine as much of the following information as possible:

(a) Whether a cybersecurity event has occurred;

(b) Assess the nature and scope of the cybersecurity event;

(c) Identify any nonpublic information that may have been involved in the cybersecurity event; and

(d) Perform or oversee reasonable measures to restore the security of the information systems compromised in the cybersecurity event in order to prevent further unauthorized acquisition, release or use of nonpublic information in the licensee's possession, custody or control.

3. If the licensee learns that a cybersecurity event has or may have occurred in a system maintained by a third-party service provider, the licensee must complete the actions listed in subsection 2 or confirm and document that the third-party service provider has completed those actions.

4. The licensee shall maintain records concerning all cybersecurity events for a period of at least 5 years from the date of the cybersecurity event and shall produce those records upon demand of the Commissioner.

Sec. 21. *1. As promptly as possible but in no event later than 72 hours after a determination that a cybersecurity event has occurred, the licensee impacted by the cybersecurity event shall notify the Commissioner of the cybersecurity event if:*

(a) This State is the licensee's state of domicile, in the case of an insurer, or this State is the licensee's home state, in the case of a licensee other than an insurer; or

(b) The licensee reasonably believes that the nonpublic information involved in the cybersecurity event is the nonpublic information of 250 or more consumers residing in this State and that the cybersecurity event is either of the following:

(1) A cybersecurity event impacting the licensee of which notice is required to be provided to any governmental body, self-regulatory agency or other supervisory body pursuant to any state or federal law; or

(2) A cybersecurity event that has a reasonable likelihood of materially harming:

(I) Any consumer residing in this State; or

(II) Any material part of the normal operation of the licensee.

2. The licensee shall provide as much of the following information as possible to the Commissioner in a form prescribed by the Commissioner:

(a) Date of the cybersecurity event.

(b) Description of how the information was exposed, lost, stolen or breached, including, without limitation, the specific roles and responsibilities of third-party service providers, if any.

(c) How the cybersecurity event was discovered.

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

(e) The identity of the source of the cybersecurity event.

(f) Whether the licensee has filed a police report or has notified any regulatory, governmental or law enforcement agencies and, if so, when such notification was provided.

(g) Description of the specific types of information acquired without authorization. Specific types of information means particular data elements, including, for example, types of medical information, types of financial information or types of information allowing identification of the consumer.

(h) The period during which the information system was compromised by the cybersecurity event.

(i) The number of total consumers in this State affected by the cybersecurity event. The licensee shall provide the best estimate in the initial report to the Commissioner and update this estimate with each subsequent report to the Commissioner pursuant to this section.

(j) The results of any internal review identifying a lapse in either automated controls or internal procedures, or confirming that all automated controls and internal procedures were followed.

(k) Description of efforts being undertaken to remediate the situation which permitted the cybersecurity event to occur.

(l) 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 event.

(m) The name of a contact person who is both familiar with the cybersecurity event and authorized to act for the licensee.

➥ A licensee shall update and supplement any information provided pursuant to this subsection if the information has materially changed or if new information becomes available.

3. A licensee shall comply with NRS 603A.220, as applicable, and provide a copy of the notice sent to consumers under that section to the Commissioner when a licensee is required to notify the Commissioner under subsection 1.

4. In the case of a cybersecurity event in a system maintained by a third-party service provider, of which the licensee has become aware, the licensee shall treat such event as it would under subsection 1 ~~(,)~~ , unless the licensee receives verification from the third-party service provider that the third-party service provider provided the notice required by subsection 1. The computation of the licensee's deadlines shall begin on the day after the third-party service provider notifies the licensee of the cybersecurity event or the licensee otherwise has actual knowledge of the cybersecurity event, whichever is sooner. Nothing in this chapter shall prevent or abrogate an agreement between a licensee and another licensee, a third-party service provider or any other party to fulfill any of the investigation requirements imposed under section 20 of this act or notice requirements imposed under this section.

5. In the case of a cybersecurity event involving nonpublic information that is used by a licensee that is acting as an assuming insurer or in the possession, custody or control of a licensee that is acting as an assuming insurer and that does not have a direct contractual relationship with the affected consumers:

(a) The assuming insurer shall notify its affected ceding insurers and the Commissioner of its state of domicile within 72 hours of making the determination that a cybersecurity event has occurred; and

(b) The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under NRS 603A.220 and any other notification requirements relating to a cybersecurity event imposed under this section.

6. In the case of a cybersecurity event involving nonpublic information that is in the possession, custody or control of a third-party service provider of a licensee that is an assuming insurer:

(a) The assuming insurer shall notify its affected ceding insurers and the Commissioner of its state of domicile within 72 hours of receiving notice from its third-party service provider that a cybersecurity event has occurred; and

(b) The ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under NRS 603A.220 and any other notification requirements relating to a cybersecurity event imposed under this section.

7. In the case of a cybersecurity event involving nonpublic information that is in the possession, custody or control of a licensee that is an insurer or its third-party service provider and for which a consumer accessed the insurer's services through an independent provider of insurance, the insurer shall notify the producers of record of all affected consumers as soon as practicable as directed by the Commissioner. The insurer is excused from this obligation for any producers who are not authorized by law or contract to sell, solicit or negotiate on behalf of the insurer, and in those instances in which ~~(it)~~ the insurer does not have the current producer of record information for any individual consumer.

Sec. 22. *1. The Commissioner may examine and investigate the affairs of any licensee to determine whether the licensee has been or is engaged in any conduct in violation of this chapter. This power is in addition to the powers which the Commissioner has under NRS 679B.120. Any such investigation or examination must be conducted pursuant to NRS 679B.230, 679B.240, 679B.250 and 679B.270 to 679B.300, inclusive.*

2. Whenever the Commissioner has reason to believe that a licensee has been or is engaged in conduct in this State which violates this chapter, the

Commissioner may take action that is necessary or appropriate to enforce the provisions of this chapter.

Sec. 23. *1. Except as otherwise provided in this section, any documents, materials or other information in the control or possession of the Division that are furnished by a licensee or an employee or agent acting on behalf of the licensee pursuant to subsection 9 of section 19 of this act or paragraphs (b) to (e), inclusive, (h), (j) or (k) of subsection 2 of section 21 of this act or that are obtained by the Commissioner in an investigation or examination pursuant to section 22 of this act are confidential by law and privileged, are not subject to disclosure pursuant to chapter 239 or 241 of NRS or NRS 679B.285, are not subject to subpoena and are not subject to discovery or admissible in evidence in any private civil action. The Commissioner may use the documents, materials or other information in the furtherance of any regulatory or legal action brought as a part of the Commissioner's duties.*

2. The Commissioner and any person who received documents, materials or other information while acting under the authority of the Commissioner must not be permitted or required to testify in any private civil action concerning any confidential documents, materials or information subject to subsection 1.

3. In order to assist in the performance of the Commissioner's duties under this chapter, the Commissioner:

(a) May share documents, materials or other information, including, without limitation, documents, materials and other information that is confidential and privileged pursuant to subsection 1, with other state, federal or 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 agrees in writing to maintain the confidentiality and privileged status of the document, material or other information;

(b) May receive documents, materials or other information, including, without limitation, otherwise confidential and privileged documents, materials or other information, from the National Association of Insurance Commissioners, its affiliates or subsidiaries and from regulatory and law enforcement officials of other foreign or domestic 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;

(c) May share documents, materials or other information subject to subsection 1, with a third-party consultant or vendor provided the consultant agrees in writing to maintain the confidentiality and privileged status of the document, material or other information; and

(d) May enter into agreements governing sharing and use of information consistent with this subsection.

4. No waiver of any applicable claim of confidentiality or privilege in the documents, materials or other information occurs as a result of disclosure to the Commissioner under this section or as a result of sharing as authorized in subsection 3.

5. Nothing in this chapter shall prohibit the Commissioner from releasing final, adjudicated actions that are open to public inspection to a database or other clearinghouse service maintained by the National Association of Insurance Commissioners, its affiliates or subsidiaries.

6. Documents, materials or other information in the possession or control of the National Association of Insurance Commissioners or a third-party consultant or vendor that are furnished by the Commissioner pursuant to

subsection 3 are confidential by law and privileged, are not subject to subpoena and are not subject to discovery or admissible in evidence in any private civil action.

Sec. 24. ***1. The following exceptions shall apply to this chapter:***

(a) A licensee ~~[with fewer than 10 employees, including any independent contractors,]~~ is exempt from section 19 of this act ~~[.]~~ :

(1) If the licensee has fewer than 10 employees, including any independent contractors.

(2) During any year in which the gross annual revenue of the licensee is less than $5,000,000.

(3) During any year in which the total assets of the licensee at the end of the year are less than $10,000,000.

(b) A licensee subject to the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, 110 Stat. 1936, enacted August 21, 1996, that has established and maintains an information security program pursuant to such statutes, rules, regulations, procedures or guidelines established thereunder, will be considered to meet the requirements of section 19 of this act, provided that licensee is compliant with, and submits a written statement certifying its compliance with, the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191, 110 Stat. 1936, and any applicable rules, regulations, procedures or guidelines established thereunder. To qualify for the exemption set forth in this paragraph, an insurer domiciled in this State must, not later than February 15 of each year for which the exemption is claimed, submit to the Commissioner the written statement required by this paragraph.

(c) An employee, agent representative or designee of a licensee, who is also a licensee, is exempt from section 19 of this act and need not develop its own information security program to the extent that the employee, agent, representative or designee is covered by the information security program of the other licensee.

2. In the event that a licensee ceases to qualify for an exemption, such a licensee shall have 180 days to comply with this chapter.

Sec. 25. ***1. The Commissioner may:***

(a) Suspend or revoke a license, certificate of authority or registration issued pursuant to this title for a violation of this chapter or any regulation adopted hereunder.

(b) In addition to the suspension or revocation of a license, certificate of authority or registration, after notice and a hearing held pursuant to NRS 679B.310 to 679B.370, inclusive, impose an administrative fine of not more than $1,000 per day for each violation or failure to comply with the provisions of this chapter, up to a maximum fine of $50,000.

(c) Adopt any regulations necessary to carry out the purposes and provisions of this chapter.

2. A licensee who is aggrieved by an administrative action taken by the Commissioner may request a hearing pursuant to NRS 679B.310 to 679B.370, inclusive.

Sec. 26. NRS 239.010 is hereby amended to read as follows:

239.010 1. Except as otherwise provided in this section and NRS 1.4683, 1.4687, 1A.110, 3.2203, 41.071, 49.095, 49.293, 62D.420, 62D.440, 62E.516, 62E.620, 62H.025, 62H.030, 62H.170, 62H.220, 62H.320, 75A.100, 75A.150, 76.160, 78.152, 80.113, 81.850, 82.183, 86.246, 86.54615, 87.515, 87.5413, 87A.200, 87A.580, 87A.640, 88.3355, 88.5927, 88.6067, 88A.345, 88A.7345, 89.045, 89.251, 90.730, 91.160, 116.757, 116A.270, 116B.880, 118B.026, 119.260, 119.265, 119.267, 119.280, 119A.280, 119A.653, 119B.370, 119B.382, 120A.690,

125.130, 125B.140, 126.141, 126.161, 126.163, 126.730, 127.007, 127.057, 127.130, 127.140, 127.2817, 128.090, 130.312, 130.712, 136.050, 159.044, 159A.044, 172.075, 172.245, 176.01249, 176.015, 176.0625, 176.09129, 176.156, 176A.630, 178.39801, 178.4715, 178.5691, 179.495, 179A.070, 179A.165, 179D.160, 200.3771, 200.3772, 200.5095, 200.604, 202.3662, 205.4651, 209.392, 209.3925, 209.419, 209.521, 211A.140, 213.010, 213.040, 213.095, 213.131, 217.105, 217.110, 217.464, 217.475, 218A.350, 218E.625, 218F.150, 218G.130, 218G.240, 218G.350, 228.270, 228.450, 228.495, 228.570, 231.069, 231.1473, 233.190, 237.300, 239.0105, 239.0113, 239B.030, 239B.040, 239B.050, 239C.140, 239C.210, 239C.230, 239C.250, 239C.270, 240.007, 241.020, 241.030, 241.039, 242.105, 244.264, 244.335, 247.540, 247.550, 247.560, 250.087, 250.130, 250.140, 250.150, 268.095, 268.490, 268.910, 271A.105, 281.195, 281.805, 281A.350, 281A.680, 281A.685, 281A.750, 281A.755, 281A.780, 284.4068, 286.110, 287.0438, 289.025, 289.080, 289.387, 289.830, 293.4855, 293.5002, 293.503, 293.504, 293.558, 293.906, 293.908, 293.910, 293B.135, 293D.510, 331.110, 332.061, 332.351, 333.333, 333.335, 338.070, 338.1379, 338.1593, 338.1725, 338.1727, 348.420, 349.597, 349.775, 353.205, 353A.049, 353A.085, 353A.100, 353C.240, 360.240, 360.247, 360.255, 360.755, 361.044, 361.610, 365.138, 366.160, 368A.180, 370.257, 370.327, 372A.080, 378.290, 378.300, 379.008, 379.1495, 385A.830, 385B.100, 387.626, 387.631, 388.1455, 388.259, 388.501, 388.503, 388.513, 388.750, 388A.247, 388A.249, 391.035, 391.120, 391.925, 392.029, 392.147, 392.264, 392.271, 392.315, 392.317, 392.325, 392.327, 392.335, 392.850, 394.167, 394.1698, 394.447, 394.460, 394.465, 396.3295, 396.405, 396.525, 396.535, 396.9685, 398A.115, 408.3885, 408.3886, 408.3888, 408.5484, 412.153, 416.070, 422.2749, 422.305, 422A.342, 422A.350, 425.400, 427A.1236, 427A.872, 432.028, 432.205, 432B.175, 432B.280, 432B.290, 432B.407, 432B.430, 432B.560, 432B.5902, 433.534, 433A.360, 437.145, 439.840, 439B.420, 440.170, 441A.195, 441A.220, 441A.230, 442.330, 442.395, 442.735, 445A.665, 445B.570, 449.209, 449.245, 449A.112, 450.140, 453.164, 453.720, 453A.610, 453A.700, 458.055, 458.280, 459.050, 459.3866, 459.555, 459.7056, 459.846, 463.120, 463.15993, 463.240, 463.3403, 463.3407, 463.790, 467.1005, 480.365, 480.940, 481.063, 481.091, 481.093, 482.170, 482.5536, 483.340, 483.363, 483.575, 483.659, 483.800, 484E.070, 485.316, 501.344, 503.452, 522.040, 534A.031, 561.285, 571.160, 584.655, 587.877, 598.0964, 598.098, 598A.110, 599B.090, 603.070, 603A.210, 604A.710, 612.265, 616B.012, 616B.015, 616B.315, 616B.350, 618.341, 618.425, 622.310, 623.131, 623A.137, 624.110, 624.265, 624.327, 625.425, 625A.185, 628.418, 628B.230, 628B.760, 629.047, 629.069, 630.133, 630.30665, 630.336, 630A.555, 631.368, 632.121, 632.125, 632.405, 633.283, 633.301, 633.524, 634.055, 634.214, 634A.185, 635.158, 636.107, 637.085, 637B.288, 638.087, 638.089, 639.2485, 639.570, 640.075, 640A.220, 640B.730, 640C.400, 640C.600, 640C.620, 640C.745, 640C.760, 640D.190, 640E.340, 641.090, 641.325, 641A.191, 641A.289, 641B.170, 641B.460, 641C.760, 641C.800, 642.524, 643.189, 644A.870, 645.180, 645.625, 645A.050, 645A.082, 645B.060, 645B.092, 645C.220, 645C.225, 645D.130, 645D.135, 645E.300, 645E.375, 645G.510, 645H.320, 645H.330, 647.0945, 647.0947, 648.033, 648.197, 649.065, 649.067, 652.228, 654.110, 656.105, 661.115, 665.130, 665.133, 669.275, 669.285, 669A.310, 671.170, 673.450, 673.480, 675.380, 676A.340, 676A.370, 677.243, 679B.122, 679B.152, 679B.159, 679B.190, 679B.285, 679B.690, 680A.270, 681A.440, 681B.260, 681B.410, 681B.540, 683A.0873, 685A.077, 686A.289, 686B.170, 686C.306, 687A.110, 687A.115, 687C.010, 688C.230, 688C.480, 688C.490, 689A.696, 692A.117, 692C.190, 692C.3507, 692C.3536, 692C.3538, 692C.354, 692C.420, 693A.480, 693A.615, 696B.550, 696C.120, 703.196, 704B.320, 704B.325, 706.1725,

706A.230, 710.159, 711.600, ***section 23 of this act and*** sections 35, 38 and 41 of chapter 478, Statutes of Nevada 2011 and section 2 of chapter 391, Statutes of Nevada 2013 and unless otherwise declared by law to be confidential, all public books and public records of a governmental entity must be open at all times during office hours to inspection by any person, and may be fully copied or an abstract or memorandum may be prepared from those public books and public records. Any such copies, abstracts or memoranda may be used to supply the general public with copies, abstracts or memoranda of the records or may be used in any other way to the advantage of the governmental entity or of the general public. This section does not supersede or in any manner affect the federal laws governing copyrights or enlarge, diminish or affect in any other manner the rights of a person in any written book or record which is copyrighted pursuant to federal law.

2. A governmental entity may not reject a book or record which is copyrighted solely because it is copyrighted.

3. A governmental entity that has legal custody or control of a public book or record shall not deny a request made pursuant to subsection 1 to inspect or copy or receive a copy of a public book or record on the basis that the requested public book or record contains information that is confidential if the governmental entity can redact, delete, conceal or separate the confidential information from the information included in the public book or record that is not otherwise confidential.

4. A person may request a copy of a public record in any medium in which the public record is readily available. An officer, employee or agent of a governmental entity who has legal custody or control of a public record:

(a) Shall not refuse to provide a copy of that public record in a readily available medium because the officer, employee or agent has already prepared or would prefer to provide the copy in a different medium.

(b) Except as otherwise provided in NRS 239.030, shall, upon request, prepare the copy of the public record and shall not require the person who has requested the copy to prepare the copy himself or herself.

Sec. 27. This act becomes effective:

1. Upon passage and approval for the purpose of adopting regulations and performing any preparatory administrative tasks that are necessary to carry out the provisions of this act; and

2. On January 1, 2020, for all other purposes.