



MIKE CHANEY
Commissioner of Insurance
State Fire Marshal

MARK HAIRE
Deputy Commissioner of Insurance

RICKY DAVIS
State Chief Deputy Fire Marshal

MISSISSIPPI INSURANCE DEPARTMENT

501 N. WEST STREET, SUITE 1001
WOOLFOLK BUILDING
JACKSON, MISSISSIPPI 39201
www.mid.ms.gov

MAILING ADDRESS
Post Office Box 79
Jackson, Mississippi 39205-0079
TELEPHONE: (601) 359-3569
FAX: (601) 359-2474

BULLETIN 2019-4 MISSISSIPPI DEPARTMENT OF INSURANCE

INSURANCE DATA SECURITY LAW SENATE BILL 2831, 2019 REGULAR SESSION

June 4, 2019

I. Purpose.

During the 2019 Regular Legislative Session, the Mississippi Legislature passed Senate Bill 2831, the Insurance Data Security Law (“Act”) which establishes the exclusive state standards applicable to Licensees for data security, the investigation of a cybersecurity event as defined in the Act, and notification to the Mississippi Insurance Department (“MID”). This Bulletin has been promulgated by the MID to provide Licensees with guidance for compliance with the Act.

II. Scope.

The Act applies to all persons who hold insurance licenses with the MID. For the purposes of the Act, out of state purchasing groups or risk retention groups are expressly exempt from the Act. *Other exemptions and exceptions may apply as discussed in Section VI of this Bulletin.*

III. Definitions

For the purposes of the Act and this Bulletin, the following definitions should be used.

- A. “Licensee” is defined as “any person licensed, authorized to operate, or registered, or required to be licensed, authorized or registered pursuant to the insurance laws of this state”.
- B. “Cybersecurity Event” is defined as “an event resulting in unauthorized access to, disruption or misuse of, an information system or nonpublic information stored on such information system”.
- C. “Third party service provider” is defined as “a person, not otherwise defined as a licensee, who contracts with a licensee to maintain, process, store or otherwise is

permitted access to nonpublic information through its provision of services to the licensee”.

D. “Nonpublic information” means electronic information that is not publicly available information and is:

1. 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 nondriver identification card number;
- c. Financial account number, credit 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;

2. 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.

IV. Requirements of Licensees.

Section 4 of the Act requires Licensees to develop, implement and maintain an information security program based on its risk assessment, with a designated employee in charge of the information security program. There are six (6) components of this Section.

- A. Risk Assessment and Implementation of Information Security Program. Licensees are required to conduct a risk assessment and then develop and maintain an information security program that is commensurate with the size and complexity of the Licensee’s business.
- B. Information Security Program Management and Maintenance. Licensees must implement security measures and designate an employee or third party vendor to be responsible for the information security program.

- C. Training and Due Diligence. Licensees are to provide cybersecurity awareness training for employees and third party vendors, and exercise due diligence with the selection of third party vendors and require them to implement the necessary security measures.
- D. Cybersecurity Event Response. Licensees shall implement an incident response plan designed to promptly respond to, and recover from, any cybersecurity event.
- E. Reporting and Certification. If a Licensee has a Board of Directors, the executive management must report to its Board in writing at least annually on the overall status of its information security program and other material matters.
- F. Annual Report. Each insurer domiciled in this state shall submit to the commissioner a written statement by February 15th, annually, certifying that the insurer is in compliance with the requirements set forth in Section 4 of the Act.

Please note that some Licensees are exempt from compliance with these requirements. See Section VI of this Bulletin for further information regarding exemptions and exceptions.

V. Cybersecurity Event Investigations.

When a Licensee learns that a cybersecurity event has or may have occurred, the Licensee, or an outside vendor or service provider retained by the Licensee, must conduct a prompt investigation.

- A. A prompt and proper investigation should, at a minimum, determine as much of the following information as possible:
 - 1. Determine whether a cybersecurity event occurred;
 - 2. Assess the nature and scope of the cybersecurity event;
 - 3. Identify any nonpublic information that may have been involved in the cybersecurity event; and,
 - 4. 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.
- B. As provided in Section 5(3) of the Act, if the Licensee learns that a cybersecurity event has or may have occurred in a system maintained by a third-party service provider, the third-party service provider may complete the steps required in Paragraph (A) of this section, and the Licensee will confirm and document that the third-party service provider has done so. *Please note that some Licensees are exempt*

from compliance with this requirement. See Section VI of this Bulletin for further information regarding exemptions and exceptions.

- C. The Licensee shall maintain records concerning all cybersecurity events for at least five (5) years from the date of the event. These records shall be produced upon demand of the Commissioner.

V. Notice of Cybersecurity Event

- A. Each Licensee shall notify the Commissioner of a cybersecurity event as promptly as possible, but in no event later than three (3) business days from a determination that a cybersecurity event involving nonpublic information has occurred when either of the following criteria has been met:
 - 1. This state is, in the case of an insurer, the state of domicile, or, in the case of a producer, the Licensee's home state, and the cybersecurity event has a reasonable likelihood of materially harming a consumer residing in this state or reasonable likelihood of materially harming any material part of the normal operations(s) of the Licensee; or
 - 2. The Licensee reasonably believes that the nonpublic information involved is of two hundred fifty (250) or more consumers residing in this state and that is either of the following:
 - a. A cybersecurity event impacting the Licensee of which notice is required to be provided to any government body, self-regulatory agency or any other supervisory body pursuant to any state or federal law; or,
 - b. 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(s) of the Licensee.
 - 3. The Licensee shall provide notice of a cybersecurity event in the manner and on a form as provided by MID. This reporting form shall be available on the MID website's Cybersecurity page by July 1, 2019.
 - 4. Licensees must comply with Miss. Code Ann. § 75-24-29, which requires any person who conducts business in this state and who, in the ordinary course of the person's business functions, owns, licenses or maintains personal information of any resident of this state, to disclose any breach of security to all affected individuals. Section 75-24-29 sets forth the requirements for providing notice of a cybersecurity event to consumers/affected individuals.

5. a. If there is a cybersecurity event in a system maintained by a third-party service provider, and the Licensee has become aware of such breach, the Licensee may allow the third-party service provider to provide the notice required.
- b. If there is a cybersecurity event in a system maintained by a third-party service provider, the computation of Licensee's deadline shall begin on the day after the third-party service provider notifies the Licensee of the cybersecurity event, or the Licensee has actual knowledge of same.

Please note that some Licensees are exempt from compliance with the requirements provided for in Section 6(4)(a) and (b) of the Act, as discussed in this subsection (5). See Section VI of this Bulletin for further information regarding exemptions and exceptions.

VI. Exemptions and Exceptions.

- A. A Licensee may be exempt from the requirements provided in Sections 4, 5(3) and 6(4)(a) and (b) of the Act if the Licensee meets any of the following criteria:
 1. Has fewer than fifty (50) employees, excluding independent contractors;
 2. Has less than Five Million Dollars (\$5,000,000.00) in gross annual revenue;
 3. Has less than Ten Million Dollars (\$10,000,000.00) in year-end total assets; or,
 4. Is an insurance producer or insurance adjuster.
- B. A Licensee that has established and maintains an information security program pursuant to the requirements of HIPAA will be considered to meet the requirements of Section 4 of the Act, provided the Licensee submits a written certification of its compliance with Section 4 of the Act.
- C. An employee, agent, representative or designee of a Licensee, who is also a Licensee, is exempt from Section 4 of the Act to the extent they are covered by the information security program of the other Licensee.
- D. A Licensee affiliated with a depository institution that maintains an Information Security Program in compliance with the *Interagency Guidelines Establishing Standards for Safeguarding Customer Information* as set forth pursuant to sections 501 and 505 of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 and 6805) shall be considered to meet the requirements of Section 4, provided that the Licensee produces, upon request, documentation satisfactory to the commissioner that independently validates the affiliated depository institution's adoption of an Information Security Program that satisfies the Interagency Guidelines.

VII. Confidentiality.

The Act provides that certain documents, materials or other information in the control or possession of MID that are furnished pursuant to the provisions of SB 2831 by a Licensee or an employee or agent acting on behalf of Licensee; or documents, materials or other information that are obtained by the MID in an investigation or examination pursuant to SB 2831 shall be confidential by law and privileged, shall not be subject to subpoena, and shall not be subject to discovery or admissible in evidence in any private civil action.

VIII. Powers of the Commissioner.


The Act grants the Commissioner the power to examine and investigate Licensees to determine compliance with the law, to issue penalties for violations of the Act in accordance with Section 83-5-85, and also provides the MID with the authority to remedy data security deficiencies should any be found during an examination.

VIX. Effective Date.

The provisions contained within this Bulletin shall be in effect on and after July 1, 2019.

The effective date of the Act is July 1, 2019. Unless exempt, Licensees shall implement Section 4 of the Act by July 1, 2020, and shall implement Section 4(6) of the Act by July 1, 2021.

Licensees are encouraged to review the Cybersecurity page at the MID website for additional materials and updated information. This information will be posted to MID's website by July 1, 2019. If there are any questions concerning this Bulletin, please contact the Department at (601) 359-3569.



MIKE CHANEY
COMMISSIONER OF INSURANCE