



# *Urgent Alert:*

## *NEW STATUTE mandates action from agents*

In 2020, the Louisiana Legislature passed the "Insurance Data Security Law" which puts new requirements on anyone with a license from the Louisiana Department of Insurance. The law has 2 primary components: the mandate for a written information security plan and mandatory investigation and reporting of any cyber breach event to the commissioner's office. Agents **MUST** be in compliance with the statute NO LATER THAN AUGUST 1, 2021, so act now!

### ***What do I need to do?***

#### **If you are an employee at an insurance agency/company/other regulated entity:**

1. Ask the owner/manager of your business to confirm that they are satisfying the requirements of the Insurance Data Security Law on your behalf.
2. See the final section below to learn about your new legal obligation to report data breaches.

#### **If you own or manage an insurance agency/company/other regulated entity or if you are self-employed in an occupation regulated by the Department of Insurance:**

Answer the following questions:

1. Does your business have fewer than 25 employees?
2. Does your business have less than \$5 million in gross annual revenue?
3. Does your business have less than \$10 million in year-end total assets?
4. Is your business subject to regulation under HIPAA or the Gramm-Leach-Bliley Act and maintaining an Information Security Program that satisfies the requirements of that act?
5. Is your business already subject to the data security laws of another jurisdiction which the Louisiana commissioner has approved as satisfying the same requirements, per the list in [this department bulletin](#)?

#### ***If you answers YES to AT LEAST ONE of those questions:***

You are exempt from the first section of the act which requires the creation of a comprehensive written information security program. You are, however, still bound by the reporting requirements of the latter part of the act (see below).

#### ***If you answered NO to ALL OF those questions:***

You must comply with ALL sections of the act and need to take immediate action. Start by reading [IIABL's Technical Advisory](#) which breaks down the law's intent and effects. IIABL's website also [offers resources](#) to begin your risk assessment and achieve compliance with the Insurance Data Security Law.

**Everyone, whether exempted from the information security plan section of the act or not, is subject to the new investigation and reporting requirements mandated by the latter part of the statute.**

- 1) If you are regulated by the Department of Insurance, you are required to investigate any potential cybersecurity event that might have affected your systems or nonpublic information stored by you or a third-party service provider.
- 2) Within 3 days of identifying the occurrence of an event, you are required to report (to the department) any cybersecurity event that has a reasonable likelihood:
  1. To harm a consumer residing in this state (for example, if nonpublic information was acquired by an unauthorized person in such a form that they might be able to use or release that information)
  2. To interrupt your normal business operations (for example, a "CryptoLocker" attack which encrypts your systems or data, denying your access)
- 3) The report should be made by sending [the department's standard reporting form](mailto:cyber.report@ldi.la.gov) to [cyber.report@ldi.la.gov](mailto:cyber.report@ldi.la.gov).

**IIABL Legal Disclaimer**

The information provided by IIABL is intended for educational and informational purposes only. IIABL does not make any warranty or representation, express or implied, with respect to the accuracy, completeness or usefulness of the information provided. Information provided represents the views of one or more experienced insurance professionals and is not a recommendation that a particular course of action be followed. Please note that this information is not legal advice upon which you should rely. Please seek any legal opinion you may need from a qualified attorney. IIABL is not liable for any liability or damage which may result from the use of this information.