Insights, News & Events

MISSOURI ADOPTS NEW DATA BREACH NOTICE LAW FOR INSURERS – THE 10 THINGS INSURERS AND LICENSED ENTITIES NEED TO KNOW

Insights
Jul 18, 2025

As cybersecurity threats escalate, state legislatures across the country are tightening requirements for how insurance entities respond to data breaches – and thanks to a new law just passed several weeks ago, Missouri is getting in on the action. On July 2, Missouri's Governor approved House Bill 974, "The Insurance Data Security Act," which will establish standards for insurers and licensed entities regarding data security, breach investigations, and notification protocols when it takes effect on January 1, 2026. What are the 10 things insurers and licensed entities need to know about this law, and where does it fit into the national picture?

The 10 Things Insurers and Licensed Entities Need to Know about the new Missouri Law

Overview of New Law

The design objectives of this new law are to:

- *Safeguard confidentiality, integrity, and security of nonpul information;*
- *Protect against threats, hazards, and unauthorized access*
- *Include a retention and destruction policy for data*

1. Information Security Program Requirements

Each licensee must develop and maintain a written information security program that:

Related People

J. Randall Coffey
Partner
816.842.8770

Daniel Pepper, CIPP/US
Partner
303.218.3661

- is tailored to the licensee's size, complexity, use of third-party providers, and the sensitivity of nonpublic information and information systems; and
- is based on a risk assessment and includes administrative, technical, and physical safeguards.

2. Oversight

The new law will assign responsibility to personnel or vendors, who will be required to identify and assess threats (both internal and external), and then evaluate current safeguards across systems and training. The law also creates an obligation to annually test key controls and systems for effectiveness.

3. Security Measures

Those covered under the law will need to implement security measures such as access controls, encryption, secure development, and multi-factor authentication, as well as to:

- maintain audit trails, and test systems for intrusion attempts; and
- include physical security, secure data disposal, and environmental hazard protections.

4. Governance and Training

Covered entities are required to include cybersecurity in their enterprise risk management program. This includes staying informed on emerging threats and also providing cybersecurity awareness training to staff.

5. Board Oversight

Executive management must maintain the security program. They must deliver annual written reports on status, compliance, and risks.

6. Third-Party Oversight

Covered entities need to not only exercise due diligence in vendor selection but require vendors to implement security measures to protect accessible data.

7. Incident Response Plan

Jillian Seifrit, CIPP/US

Associate

610.230.6129

Service Focus

Data Protection and Cybersecurity

Privacy and Cyber

Related Offices

Kansas City

Each licensee must develop a plan to:

- respond to cybersecurity events;
- define roles, goals, communication strategy, and remediation steps; and
- document events and revise the plan as needed.

8. Investigation Requirements

When a licensee learns of a possible cybersecurity event, it must promptly:

- investigate whether an event occurred;
- assess scope and impact, including which types of nonpublic information were involved; and
- take remedial action to secure affected systems and prevent further unauthorized access.

If the breach involves a third-party provider, the licensee must either complete the investigation itself or confirm the provider has done so. Finally, licensees must maintain records of cybersecurity events for three years and produce them upon request from the Missouri Director of the Department of Commerce and Insurance.

9. Notification Requirements

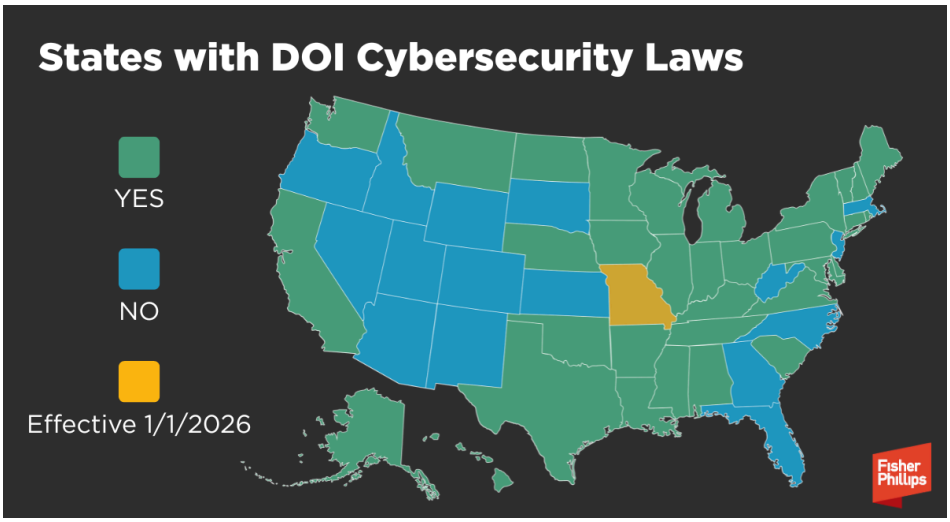
Licensees must notify the Insurance Director within **four business days** when a cybersecurity event involving nonpublic information has occurred when either:

- Missouri is the licensee's state of domicile or an insurer's home state, **and** the cybersecurity event has a reasonable likelihood of materially harming a Missouri resident **or** a reasonable likelihood of materially harming normal business operations; **OR**
- The licensee reasonably believes that **250+** Missouri consumers' nonpublic information is involved **and**
  - Requires reporting to any other state or federal law regulatory, **or**
  - Has a reasonable likelihood of harming a Missouri consumer or business operations.

10. Special Cases and Third-Party Events

If a third-party service provider's system is breached, the licensee must treat it as its own incident. The notification deadlines start when the licensee is notified or becomes aware, and agreements between parties may delegate investigation and notification duties.

National Trends and Comparative Insights



Missouri will join 32 other states and Puerto Rico with DOI specific notice requirements, a clear signal of the growing momentum behind stricter cybersecurity regulations across the US for insurance entities. Further, there is also pending legislation in Idaho.

The majority of these states, along with Missouri, utilize the National Association of Insurance Commissioners (NAIC) Insurance Data Security Model Law. The model law's key provisions are:

Core Requirements

- Information Security Program: Licensees must create and maintain a security program tailored to their risk profile, with a designated employee overseeing it.
- Risk Assessment: Ongoing evaluations of internal and external threats guide the security measures implemented.
- Third-Party Oversight: Ensure that vendors and service providers also meet security standards, with phased compliance timelines.

Cybersecurity Event Response

- Investigation: Any suspected cybersecurity event must be promptly investigated to determine its scope and impact.
- Notification: If an event meets certain thresholds, the licensee must notify the state insurance commissioner, typically within 72 hours.

Regulatory Authority

- Examinations: Insurance commissioners can audit and investigate licensees to ensure compliance.
- Remediation Powers: Regulators are empowered to address and correct any deficiencies uncovered during these examinations.

These DOI requirements are separate and in addition to the existing data breach statute requirements in all states, but they raise the bar significantly. What sets them apart? Accelerated reporting timelines, more stringent compliance standards, and a broader definition of nonpublic information that goes beyond most states' definitions of personally identifiable information.

Conclusion

We'll continue monitoring developments and provide updates, so make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information. If you have questions, contact your Fisher Phillips attorney, the authors of this Insight, any attorney in our Kansas City office, or any attorney on our Data Protection and Cybersecurity team.