

SB 134 - Insurance Data Security

Sponsored by Senator Kaufman

Presented by Dominick Harnett – Staff to Sen. Kaufman

Senate Labor & Commerce Committee

February 5th, 2024

Why this matters

- In recent years, there have been dozens of major data breaches involving large insurers that have exposed and compromised the sensitive personal information of millions of insurance costumers
- Cyber-attacks in the insurance sector are growing exponentially as more companies move to digitize their businesses. While this comes with plenty of benefits to consumers and insurance companies alike, it also introduces new cyber-risks and avenues for cyber-criminals to exploit vulnerabilities in the complex systems
- Specific to healthcare, in 2023 more than 540 organizations and 112 million individuals were implicated in healthcare data breaches reported to the HHS Office for Civil Rights (OCR). Some examples include:
 - Perry Johnson & Associates (PJ&A) disclosed a May data breach to impacted healthcare organization clients in November
 - Managed Care of North America (MCNA), a dental benefits administrator that provides services to Medicaid and CHIP programs across eight states, suffered a major healthcare data breach between February and March
 - Healthcare company, Welltok, notified nearly 8.5 million individuals of a data breach stemming from the May 2023 MOVEit hack
 - PharMerica disclosed a breach to OCR in May that impacted more than 5.8 million individuals

- National Association of Insurance Commissioners (NAIC) Model law
- Law sets standards intended to reduce potential damage of data breaches within the Industry
- Applies to insurers licensed by the state with exemptions
- US Treasury has urged states to adopt the model law or they will ask Congress to preempt the states

What SB 134 Does

- Requires companies licensed by the Division of Insurance to maintain an information security program based on risk assessments with a designated employee in charge of the program
- Sets investigative and notification requirements when a cybersecurity event occurs
- Grants the director of the Division of Insurance the authority to examine compliance by licensees and the means to remedy deficiencies found during examination