OLR Bill Analysis

sHB 6391

AN ACT CONCERNING THE INSURANCE DEPARTMENT'S RECOMMENDATIONS REGARDING THE GENERAL STATUTES.

SUMMARY

This bill makes changes to the adverse determination process, including (1) eliminating a filing fee for external and expedited external adverse determination reviews and (2) requiring health carriers, and not the commissioner, to notify covered individuals about these reviews.

The bill also makes several changes to the Insurance Data Security Law, which generally requires insurers and other entities regulated by the insurance department to inform the department and insureds of cybersecurity breaches. Among other changes to the data security law, the bill:

1. clarifies that the law's scope is limited to breaches of nonpublic information;

2. delays implementation of several provisions by one year;

3. imposes deadlines by which certain exempt entities must submit certification to the commissioner; and

4. changes which entities must notify the commissioner and insureds, and the circumstances under which they must do so.

The bill requires health care centers (i.e., HMOs) and insurers to provide documentation to the insurance commissioner, upon his request, substantiating the number of lives they cover or insure as annually reported. Under the bill, the commissioner may fine HMOs and insurers (1) who fail to comply by the statutory deadline or (2) if he finds data discrepancies not attributable to good faith mistakes.

The bill repeals a requirement for the insurance commissioner to annually submit a report to the Insurance and Real Estate Committee containing information he has received related to (1) fires caused by arson, (2) workers' compensation fraud unit quarterly reports, (3) motor vehicle insurance fraud, and (4) health insurance fraud (§ 2).

Lastly, the bill allows insurers, in their discretion, to pay the insurance fund assessment at once when the first installment is due on June 30, instead of quarterly (§ 4). (By law, the insurance department assesses domestic insurers to fund the department, Office of Health Strategy, Office of Healthcare Advocate, and the Department of Rehabilitation Services' fall prevention program.)

The bill also makes minor, technical, and conforming changes.

EFFECTIVE DATE: July 1, 2021, except the provisions changing the data security law and repealing the insurance commissioner reporting requirement are effective upon passage, and the adverse determination provisions are effective October 1, 2021.

§ 5 — EXTERNAL REVIEW PROCESS

Filing Fee

The bill eliminates the $25 filing fee that must accompany a request for an external or expedited external adverse determination review. Under current law, the fee is (1) waived if the commissioner finds the covered person is indigent or unable to pay, and (2) returned if the review is overturned.

Process and Deadlines

The bill requires the commissioner to assign an independent review organization (IRO) within one business day after receiving a complete request for expedited external adverse determination review, instead of one calendar day after it. Existing law requires him to meet this same deadline for external adverse determination reviews that are not expedited.

The bill also requires health carriers, instead of the commissioner, to notify covered individuals or their representatives of (1) an accepted

external or expedited external adverse determination request and (2) where and how to send additional information. The bill also requires health carriers to notify the commissioner. By law, a covered person or their representative must be notified that they may submit additional information to the IRO within five business days. An IRO must consider any information it receives in this timeframe and may consider information received after it. (Existing law requires carriers to notify the commissioner and the covered individual of whether the review is accepted within one business day.)

Lastly, the bill requires health carriers to provide the necessary health information to the IRO within five business days (for an external review) or one calendar day (for an expedited external review), beginning when they accept the review instead of when they receive the IRO's name from the commissioner.

§ 3 — DATA SECURITY LAW

The bill makes several changes to the state Insurance Data Security Law (CGS § 38a-38).

Applicability

The bill clarifies that the insurance data security law only applies to cyber security events resulting in unauthorized access to nonpublic, rather than any, information. Under current law, "nonpublic information" is information that is not publicly available and that:

1. concerns a consumer's name, number, or other identifiable information that can identify a consumer when used in combination with an access or security code to a consumer's financial account; account, credit, or debit card number; biometric records; driver's license or nondriver identification number; or Social Security number;

2. would materially impact a licensee's business, operation, or security if disclosed or used without authorization; or

3. is created or derived from a consumer or health care provider and concerns behavioral, mental, or physical health, or health

care services or payments.

Under the bill, nonpublic information is electronic data and information that meets the above criteria. As under existing law, nonpublic information excludes a consumer's age or gender.

The bill also explicitly applies the law's requirements to fraternal benefit societies, interlocal risk management agencies, or employers' mutual associations. (These organizations are exempt from certain other insurance laws.) But it exempts from the law any Superior Court commissioner acting as a title agent.

New York Requirement Compliance. Under current law, licensees that comply with another jurisdiction approved by the commissioner and annually submit to the commissioner a written statement certifying compliance are deemed to have satisfied data security requirements. The bill limits this so that only licensees that comply with New York's Cybersecurity Requirements for Financial Services Companies regulations (23 NYCRR 500) are deemed to have satisfied the law's requirements. The bill also moves the deadline for the annual written statement from February 15 to April 15.

Annual Certification

The bill requires domiciled health care centers and fraternal benefit societies, including those that are part of an insurance holding company system, to comply with the law's annual certification, record retention, and remediation requirements.

Certification and Record Retention. By law, insurers and others covered by the bill and law must submit to the commissioner a written statement certifying that the insurer has complied with the law's risk assessment and information security program provisions. Each applicable entity must maintain all supporting documents for examination, including data, records, and schedules, for at least five years after submitting its certification. For all covered entities, the bill requires this certification by April 15, instead of February 15.

The bill also allows a domestic insurer, HMO, or fraternal benefit

society that is a member of an insurance holding company system to submit one certification statement on behalf of all the holding company members.

Remediation. Existing law requires insurers that identify areas, processes, or systems that require material improvements, redesigns, or updates to (1) document and identify the remediation efforts planned and underway and (2) make the documents available to the commissioner on request. The bill extends this requirement to HMOs and fraternal benefit societies and specifies that companies may comply directly or through an affiliate.

Delayed Implementation

The bill delays by one year, until October 1, 2021, the deadline for insurers and other covered entities to implement an information security program. By law, information security programs must, among other things, (1) contain administrative, technical, and physical safeguards to protect nonpublic information and the company's information systems and (2) define, and periodically reevaluate, a schedule for retaining nonpublic information and a mechanism to destroy this information when it is no longer needed.

It also delays, by one year, until October 1, 2022, the date by which insurers and other covered entities must require third-party service providers to implement appropriate measures to protect data and nonpublic information.

It also delays, by one year, the period during which certain small licensees are exempt from the law's requirements. Current law exempts (1) from October 1, 2020, to September 30, 2021, licensees with fewer than 20 employees and (2) after October 1, 2021, licensees with fewer than 10 employees. Under the bill, the exempt periods are October 1, 2021, to September 30, 2022, and after October 1, 2022, respectively.

HIPAA Certification

Licensees subject to, and that certify to the commissioner they

comply with, the federal Health Insurance Portability and Accountability Act are deemed to have satisfied the state data security requirements. The bill requires this certification to be submitted annually by April 15.

Cyber Security Event Notification

Current law requires licensees to notify the commissioner within three business days after a cybersecurity event and report certain related information. The bill specifies that a licensee must notify the commissioner within three business days after first determining that a cybersecurity event occurred and correspondingly adds the date on which the cybersecurity event was discovered to the information that must be reported.

It also requires the licensee to report the total number of consumers residing in Connecticut that, to the licensee's knowledge at the time of the report, are impacted by the cybersecurity event. Current law requires a licensee to report the total number of impacted Connecticut consumers.

Under current law, certain licensed insurance producers and domestic insurers must notify the insurance commissioner of a cyber security event if they:

1. reasonably believe that the nonpublic information involved in the cybersecurity event affects at least 250 Connecticut residents and

2. (a) must send a cybersecurity notice to any governing, regulatory, or supervisory body under federal or state law or (b) it is reasonably likely the cybersecurity event will materially harm a Connecticut consumer or the licensee's business.

The bill establishes different reporting requirements for domestic insurers and Connecticut insurance producers. These entities must report a cybersecurity event if it is reasonably likely that the event will materially harm a Connecticut consumer or the licensee's business.

The bill extends existing notification requirements to any licensee that:

1. reasonably believes that the nonpublic information involved in the cybersecurity event affects at least 250 Connecticut residents and

2. (a) must send a cybersecurity notice to any governing, regulatory, or supervisory body under federal or state law or (b) it is reasonably likely the cybersecurity event will materially harm any Connecticut consumer or the licensee's business.

The bill also changes how the reporting deadline is calculated for cybersecurity events of third-party service providers. Under the bill, it begins with the first day after a licensee has actual knowledge of a cybersecurity event, instead of when they become aware of it.

Confidential Information

By law, material and other information provided to the commissioner is confidential and privileged, and exempt from disclosure under the state's Freedom of Information Act and any subpoena or discovery in a private cause of action. However, the commissioner may share this information with certain other parties, including the National Association of Insurance Commissioners (NAIC). The bill extends this confidentiality to all materials and information provided to, or in custody or control of, NAIC or a third-party consultant.

Commissioner Authority

The bill allows the commissioner to, after a hearing, take any action necessary or appropriate to enforce the law's provisions. By law, he may suspend or revoke a license and impose a civil fine, among other actions.

§ 1 — REPORTING REQUIREMENTS AND PENALTIES

By law, all domestic HMOs and insurers must report annually to the commissioner on the number of Connecticut lives they insure or enroll. This data is used to calculate the public health fee they must pay. The

bill allows the commissioner to require each HMO or insurer, or any other appropriate person, to submit any records the HMO, insurer, or person possesses that were used to prepare the annual report.

The bill allows the commissioner to assess an insurer or HMO a civil fine of up to $15,000 if he determines that there is a discrepancy, other than in good faith, between the actual number of covered lives and the reported number. By law, anyone aggrieved by a commissioner's decision may request a hearing and, if necessary, appeal the decision to Superior Court under the Uniform Administrative Procedure Act (CGS § 38a-19).

The bill also establishes a $100 per day penalty, in a form and manner the commissioner prescribes, for failing to submit the report by the statutorily required September 1 deadline.

These provisions are applicable to HMOs and insurers that provide policies covering (1) basic hospital expenses; (2) basic medical-surgical expenses; (3) major medical expenses; or (4) hospital or medical services, including those provided under an HMO plan.

COMMITTEE ACTION

Insurance and Real Estate Committee

Joint Favorable Substitute
Yea 18 Nay 0 (03/22/2021)