Alaska State Legislature

SESSION:
Alaska State Capitol
Juneau, AK 99801
(907) 465-4949

INTERIM
1500 W Benson Blvd
Anchorage, AK 99503
(907) 269-0244

SENATOR JAMES KAUFMAN

Sectional Analysis for SB 134 – Version H

"An Act relating to insurance; relating to insurance data security; relating to mammograms; amending Rule 26, Alaska Rules of Civil Procedure, and Rules 402 and 501, Alaska Rules of Evidence; and providing for an effective date."

Section 1:

AS 21.23 is amended by adding new sections to Article 2 related to Insurance Data Security.

Sec. 21.23.240. Purpose and construction

Specifies the purpose of the bill to establish an exclusive state standard and clarifies that this bill does not prevent a private cause of action.

Sec. 21.23.250. Risk Assessment

Licensees shall conduct a risk assessment commensurate with the size and complexity of the licensee.

- In conducting the risk assessment, the licensee shall identify reasonably foreseeable internal and external threats, assess the likelihood and potential damage of threats, and assess the sufficiency of current safeguards in protecting nonpublic information.
- A licensee shall use this risk assessment to design the information security program required in the next section.

Sec. 21.23.260. Information Security Program

Licensees shall develop, implement, and maintain an information security program.

- The program is to be based off the threats identified in Sec 21.23.250
    - Licensees shall designate one or more employees, an outside vendor, or third-party service provider to be responsible for the security program.
    - A licensee's information security program must:
        - Contain safeguards to protect security and confidentiality of nonpublic information and the information system.
        - Protect against threats, hazards, and unauthorized access to nonpublic information.
        - Establish a schedule for retention of nonpublic information.
        - Establish a mechanism for secure destruction of nonpublic information.

Sen.James.Kaufman@akleg.gov

- The development and upkeep process of the licensee's information security program shall:
  - Implement appropriate security measures such as information access controls, identification and management of data access points, physical access controls, encryption, secure development practices, regular tests, audit trails, disaster responses, and secure disposal.
  - Determine cybersecurity risks to include in the licensee's risk management process.
  - Stay informed of emerging threats or vulnerabilities.
  - Include cybersecurity risks in the licensee's enterprise-wide risk management process.
  - Provide personnel with cybersecurity awareness training.
  - Implement information safeguards addressing identified threats and annually assess effectiveness of safeguards.
  - Exercise due diligence in the third-party service provider selection process including testing of externally developed applications.
  - Monitor, evaluate, and adjust the information security program as appropriate.
  - Establish a written incident response plan for responding to a cybersecurity event that addresses.
    - Internal response processes
    - Goals of the plan
    - Roles, responsibilities, and decision authority
    - Internal processes for communication and information sharing
    - Plans for how to remediate identified weaknesses
    - Documentation and reporting of cybersecurity events
    - Evaluation and revision process of incident response plan
- Requires the licensee board to delegate responsibility of the program to executive management which is required to at least once a year develop a report that:
  - Provides overall status of the information security program and compliance with the contents of this bill.
  - Material matters related to the information security program such as assessments, decisions, test results, cybersecurity events, and more.
- If the executive management uses a delegate to implement the program, the executive management is required to oversee the development of the program by the delegate.
- 21.23.260(f) sets requirements for licensees domiciled in the state to submit annual reports to the Director of Insurance certifying that the licensee complies with this section and the previous section, including keeping records for at least five years.

Sec. 21.23.270. Investigation of cybersecurity event

Sets investigating requirements for licensees when a cybersecurity event occurs.

- If a cybersecurity event occurs, the licensee or responsible party shall investigate the event and assess the nature and scope of the event, identify nonpublic information involved, restore the security of the information systems that were compromised, and retain relevant information for a period of at least 5 years.

Sen.James.Kaufman@akleg.gov

Sec. 21.23.280. Notification of cybersecurity event

Sets notification criteria for licensees when a cybersecurity event occurs.

- Licensees must notify the director of insurance within three business days of a cybersecurity event occurring unless federal law enforcement instructs otherwise. Licensees are affected if:
  - They are insurers domiciled in the state.
  - They are insurance producers in which Alaska is their home state.
  - The cybersecurity event involves nonpublic information of 250 or more consumers and:
    - State or federal law requires notice to a government agency.
    - There is a reasonable likelihood of materially harming a consumer in the state or the licensee's normal operations.
- The report to the director of insurance must include to the extent possible information specified in AS 21.23.280(b) in a form and format as prescribed by the director.
- 21.23.280(e) allows notification period to begin one day after the licensee is made aware of a cybersecurity event affecting information systems maintained by third-party service providers.
- 21.23.280(f) sets requirements and standards for assuming insurers to notify affected ceding insurers and the appropriate supervisory official of the licensee's state of domicile.
- 21.23.280(j) sets reporting standards for insurers and insurance producers.

Sec. 21.23.290. Confidentiality

Establishes that all information shared with the Division by licensees remains strictly confidential. This means that the information is:

- not subject to inspection and copying under AS 40.25.110
- not obtainable by subpoena or discovery
- not admissible in evidence in private civil action

21.23.290(b), (c), (d), (e) gives privileges to the director when using documents, materials, or information as described earlier in this section when done in the performance of the duties of the director.

Sec. 21.23.300. Applicability

This section establishes the criteria for which licensees are not subject to the provisions set by this bill.

- Licensee with fewer than 10 employees
- Licensees that are employees, agents, representatives, or designees of another licensee that is already covered by an information security program.
- Licensee is subject to and in compliance with the Health Insurance Portability and Accountability Act of 1996 (P.L. 104-191)

Sen.James.Kaufman@akleg.gov

Sec. 21.23.310. Enforcement; penalties

In addition to the powers of examination and investigation given to the director under AS 21.06.120, the director may take necessary or appropriate action to enforce previous sections of this act.

Sec. 21.23.399. Definitions

Adds selected definitions.

Section 2:
Amends AS 21.42.375(e) to define "diagnostic breast examination" and "supplemental breast examination" and offers guidelines for the basis of additional testing.

Section 3:
Adds a new subsection to AS 21.42.375 guaranteeing that mammography screening, diagnostic breast examinations, and supplemental breast examinations are covered by applicable insurance plans, with the exception of high deductible health plans that are eligible for a health savings account tax deduction.

Section 4:
Rule 26, 402, and 501 Alaska Rules of evidence changes.

- Rules 26 - Prohibits discovery of evidence in the possession or control of the division of insurance that was provided by a licensee under AS 21.23.260(f) or 21.23.280(b)(2)-(5), (8), (10), or (11) or that is obtained by the director in an investigation or examination under AS 21.23.310.
- Rule 402 and 501 – AS 21.23.290(a)(4) and (c) enacted in Sec. 1 of this Act prevent the director of the division of insurance acting under the authority of the director from being compelled to testify about confidential or privileged documents. It also precludes admissibility of evidence in a private action of documents, materials, or other privileged information.

Section 5:
Amends the law of the State of Alaska by applying Sec. 2 and Sec. 3 to an insurance policy or contract on or after the effective date of the law.

Section 6:
This section notices the Division to begin the process of writing regulations but does not implement any before the effective date in Sec. 8 of this Act.

Section 7:
A conditional effect for AS 21.23.290(a)(3) and (4) and (c) enacted by Sec. 1 of this bill requires a two-thirds majority vote of each house as required for court rules changes required by art. IV, sec. 15, of the Constitution of the State of Alaska.

Section 8:
Sec.6 takes effect immediately so that the Division of Insurance can start drafting regulations.

Sen.James.Kaufman@akleg.gov

Section 9:
Sets an effective date of January 1, 2025 for several provisions in AS 21.23.290 (Confidentiality).

Section 10:
Sets an effective date of January 1, 2026 for provisions in AS 21.23.250 and AS 21.23.260.

Section 11:
Sets an effective date of January 1, 2027 for insurance companies using a third-party service provider.

Section 12:
Except as provided in secs. 5 – 8 of this bill, this Act takes effect January 1, 2025.

Sen.James.Kaufman@akleg.gov