



# LAWS OF ALASKA

2024

**Source**

HCS CSSB 134(JUD)

**Chapter No.**

\_\_\_\_\_

**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.

\_\_\_\_\_

**BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF ALASKA:**

THE ACT FOLLOWS ON PAGE 1



**AN ACT**

1 Relating to insurance; relating to insurance data security; relating to mammograms; amending  
2 Rule 26, Alaska Rules of Civil Procedure, and Rules 402 and 501, Alaska Rules of Evidence;  
3 and providing for an effective date.

4

5 \* **Section 1.** AS 21.23 is amended by adding new sections to read:

6

**Article 2. Insurance Data Security.**

7

**Sec. 21.23.240. Purpose and construction.** (a) AS 21.23.240 - 21.23.399  
8 establish the exclusive state standard for data security for licensees and govern the  
9 investigation and notification of a cybersecurity event.

10

(b) AS 21.23.240 - 21.23.399 may not be construed to

11

(1) create or imply a private cause of action for violation of  
12 AS 21.23.240 - 21.23.399; or

13

(2) prevent a private cause of action that would otherwise exist in the  
14 absence of AS 21.23.240 - 21.23.399.

1           **Sec. 21.23.250. Risk assessment.** (a) A licensee shall conduct a risk  
2 assessment commensurate with the size and complexity of the licensee and in  
3 consideration of the nature and scope of the licensee's activities to evaluate the  
4 security and confidentiality of nonpublic information used by or in the possession or  
5 control of the licensee. In conducting the risk assessment, the licensee shall

6                   (1) identify reasonably foreseeable internal or external threats in each  
7 area of the licensee's operations that could result in unauthorized access, transmission,  
8 disclosure, misuse, alteration, or destruction of nonpublic information, including the  
9 security of information systems and nonpublic information that are accessible to, or  
10 held by, third-party service providers;

11                   (2) assess the likelihood and potential damage of the threats identified  
12 in (1) of this subsection, taking into consideration the sensitivity of nonpublic  
13 information; and

14                   (3) assess the sufficiency in each area of the licensee's operations of  
15 the licensee's policies, procedures, information systems, and other safeguards in place  
16 to manage the threats identified in (1) of this subsection, including the areas of

17                           (A) employee training and management;

18                           (B) network and software design, information classification,  
19 governance, processing, storage, transmission, and disposal; and

20                           (C) detecting, preventing, and responding to attacks or  
21 intrusions on information systems and nonpublic information, or other  
22 information system failures.

23           (b) A licensee shall use the licensee's risk assessment to design the licensee's  
24 information security program required under AS 21.23.260(a).

25           **Sec. 21.23.260. Information security program.** (a) A licensee shall develop,  
26 implement, and maintain a comprehensive written information security program based  
27 on the licensee's risk assessment conducted under AS 21.23.250(a). A licensee shall  
28 designate one or more employees, an outside vendor, or a third-party service provider  
29 to act on behalf of the licensee as the person responsible for the licensee's information  
30 security program.

31                   (b) A licensee's information security program must

1 (1) contain administrative, technical, and physical safeguards to protect  
2 the security and confidentiality of nonpublic information and the security of the  
3 licensee's information system;

4 (2) protect against a threat or hazard to the security or integrity of  
5 nonpublic information and the information system;

6 (3) protect against unauthorized access to or use of nonpublic  
7 information and minimize the likelihood of harm to a consumer;

8 (4) establish and periodically reevaluate a schedule for retention of  
9 nonpublic information; and

10 (5) establish and implement a mechanism for the destruction of  
11 nonpublic information when the information is no longer needed.

12 (c) In developing, implementing, and maintaining a licensee's information  
13 security program, the licensee shall

14 (1) based on the licensee's risk assessment conducted under  
15 AS 21.23.250(a), implement the following security measures if the licensee  
16 determines that the security measure is appropriate:

17 (A) place and use effective access controls on information  
18 systems, including controls to authenticate and permit access only by  
19 authorized individuals, to protect against the unauthorized acquisition of  
20 nonpublic information; the controls may include multi-factor authentication  
21 procedures;

22 (B) identify and manage the data, personnel, devices,  
23 information systems, and facilities that enable the organization to achieve its  
24 business objectives in accordance with the relative importance of the data,  
25 personnel, devices, information systems, and facilities to the organization's  
26 business objectives and risk strategy;

27 (C) allow only authorized individuals to access physical  
28 locations containing nonpublic information;

29 (D) protect by encryption or other appropriate means nonpublic  
30 information transmitted over an external network or stored on a laptop  
31 computer or other portable computing or storage device or media;

1 (E) adopt secure development practices for applications used  
2 by the licensee that are developed in-house; the licensee shall adopt procedures  
3 for testing the security of externally developed applications used by the  
4 licensee;

5 (F) modify information systems in accordance with the  
6 licensee's information security program;

7 (G) regularly test and monitor information systems and  
8 procedures to detect actual and attempted attacks on, or intrusions into,  
9 information systems;

10 (H) include audit trails inside the information security program  
11 that are designed to detect and respond to cybersecurity events and to  
12 reconstruct material financial transactions sufficient to support normal  
13 operations and obligations of the licensee;

14 (I) implement measures to protect against destruction, loss, or  
15 damage of nonpublic information caused by environmental hazards, including  
16 fire and water damage, or other catastrophes or technological failures; and

17 (J) develop, implement, and maintain procedures for the secure  
18 disposal of nonpublic information in any format;

19 (2) determine the cybersecurity risks to include in the licensee's risk  
20 management process;

21 (3) stay informed of emerging threats or vulnerabilities and, when  
22 sharing information, use reasonable security measures in accordance with the  
23 character of the sharing and the type of information shared;

24 (4) include cybersecurity risks in the licensee's enterprise risk  
25 management process;

26 (5) provide personnel of the licensee with cybersecurity awareness  
27 training that is updated as necessary to reflect the risks identified in the risk  
28 assessment;

29 (6) implement information safeguards to manage the threats identified  
30 in a risk assessment, and, not less than once a year, assess the effectiveness of the key  
31 controls, information systems, and procedures of the safeguards;

1 (7) exercise due diligence in selecting a third-party service provider;

2 (8) where appropriate, require a third-party service provider to  
3 implement appropriate administrative, technical, and physical measures to protect and  
4 secure the information systems and nonpublic information that are accessible to, or  
5 held by, the third-party service provider; for purposes of this paragraph, encrypted  
6 nonpublic information is not considered accessible to, or held by, the third-party  
7 service provider if the associated protective process or key necessary to assign  
8 meaning to the nonpublic information is not within the possession of the third-party  
9 service provider;

10 (9) require that a third-party service provider that has access to or  
11 holds nonpublic information notify the licensee as soon as possible but not later than  
12 10 business days after determining that the third-party service provider has  
13 experienced a cybersecurity event involving nonpublic information associated with a  
14 consumer; for purposes of this paragraph, encrypted nonpublic information is  
15 considered accessible to or held by the third-party service provider if the associated  
16 protective process or key necessary to assign meaning to the nonpublic information is  
17 within the possession of the third-party service provider;

18 (10) monitor, evaluate, and adjust, as appropriate, the information  
19 security program consistent with relevant changes in technology, the sensitivity of its  
20 nonpublic information, internal or external threats to nonpublic information, and the  
21 licensee's own changing business arrangements, including mergers, acquisitions,  
22 alliances, joint ventures, outsourcing arrangements, and changes to information  
23 systems; and

24 (11) establish a written incident response plan designed to promptly  
25 respond to, and recover from, a cybersecurity event that compromises the  
26 confidentiality, integrity, or availability of nonpublic information in the licensee's  
27 possession, the licensee's information systems, or the continuing functionality of an  
28 aspect of the licensee's business or operations; the incident response plan must address  
29 the following:

30 (A) the internal process for responding to a cybersecurity  
31 event;

- 1 (B) the goals of the incident response plan;
- 2 (C) the definition of clear roles, responsibilities, and levels of  
3 decision-making authority;
- 4 (D) the licensee's internal process used for external and internal  
5 communication and information sharing;
- 6 (E) the identification of requirements for the remediation of an  
7 identified weakness in information systems and associated controls;
- 8 (F) the documentation and reporting of cybersecurity events  
9 and related incident response activities; and
- 10 (G) the evaluation and revision as necessary of the incident  
11 response plan following a cybersecurity event.

12 (d) A licensee's board of directors or an appropriate committee of the  
13 licensee's board of directors shall, at a minimum, require that

14 (1) the licensee's executive management or the executive  
15 management's delegate develop, implement, and maintain the licensee's information  
16 security program; and

17 (2) at least once a year, the licensee's executive management or the  
18 executive management's delegate report to the licensee's board of directors or an  
19 appropriate committee of the licensee's board of directors the following in writing:

20 (A) the overall status of the information security program and  
21 the licensee's compliance with AS 21.23.240 - 21.23.399; and

22 (B) material matters related to the information security  
23 program, including risk assessment, risk management and control decisions,  
24 third-party service provider arrangements, results of testing, cybersecurity  
25 events or violations, management's responses to the cybersecurity events or  
26 violations, and recommendations for changes in the information security  
27 program.

28 (e) If a licensee's executive management meets a requirement under (d) of this  
29 section through a delegate, the executive management shall oversee the development,  
30 implementation, and maintenance of the licensee's information security program  
31 prepared by the delegate. The delegate shall provide a report to the executive



1 management that complies with the requirements of (d)(2) of this section.

2 (f) Each licensee who is an insurer domiciled in this state shall

3 (1) submit to the director a written statement by February 15 of each  
4 year certifying that the insurer is in compliance with the requirements under  
5 AS 21.23.250 and this section;

6 (2) maintain and allow the director to examine for a period of five  
7 years after the insurer submits the written statement described in (1) of this subsection  
8 all records, schedules, and data supporting the written statement; and

9 (3) provide documentation of any areas, information systems, or  
10 processes that the insurer has identified as requiring material improvement, updating,  
11 or redesign, and provide documentation of the remedial efforts planned and underway  
12 to address the areas, information systems, or processes; the insurer shall make the  
13 documentation available for examination by the director at the director's request.

14 (g) In this section,

15 (1) "authorized individual" means an individual known to and screened  
16 by the licensee and for whom the licensee has determined access to the nonpublic  
17 information held by the licensee and its information systems is appropriate and  
18 necessary;

19 (2) "multi-factor authentication" means authentication through  
20 verification of at least two of the following types of authentication factors:

21 (A) a knowledge factor, including a password;

22 (B) a possession factor, including a token or text message on a  
23 mobile telephone; or

24 (C) an inherence factor, including a biometric characteristic.

25 **Sec. 21.23.270. Investigation of cybersecurity event.** (a) If a licensee  
26 becomes aware that a cybersecurity event has or may have occurred, the licensee or an  
27 outside vendor or third-party service provider designated to act on behalf of the  
28 licensee shall promptly investigate the cybersecurity event. During the investigation, if  
29 the licensee, outside vendor, or third-party service provider determines that a  
30 cybersecurity event has occurred, the licensee, outside vendor, or third-party service  
31 provider shall, to the extent possible,

1 (1) assess the nature and scope of the cybersecurity event;  
2 (2) identify nonpublic information that may have been involved in the  
3 cybersecurity event; and

4 (3) perform or oversee reasonable measures to restore the security of  
5 the information systems compromised in the cybersecurity event to prevent further  
6 unauthorized acquisition, release, or use of nonpublic information in the licensee's  
7 possession or control.

8 (b) If a licensee becomes aware that a cybersecurity event has or may have  
9 occurred in an information system maintained by a third-party service provider, the  
10 licensee shall, to the extent possible, complete the actions described in (a) of this  
11 section or confirm and document that the third-party service provider has completed  
12 those actions.

13 (c) A licensee shall maintain records concerning all cybersecurity events for a  
14 period of at least five years from the date of the cybersecurity event and shall produce  
15 the records at the request of the director.

16 **Sec. 21.23.280. Notification of cybersecurity event.** (a) Unless a federal law  
17 enforcement official instructs the licensee not to distribute information regarding a  
18 cybersecurity event, a licensee shall notify the director as soon as possible and not  
19 later than three business days after the licensee determines that a cybersecurity event  
20 has occurred, if

21 (1) the licensee is an insurer and domiciled in this state;

22 (2) the licensee is an insurance producer and this state is the licensee's  
23 home state as defined in AS 21.27.990; or

24 (3) the licensee reasonably believes that the cybersecurity event  
25 involves the nonpublic information of 250 or more consumers residing in this state and  
26 the cybersecurity event

27 (A) affects the licensee, and a state or federal law requires the  
28 licensee to provide notice of the cybersecurity event to a government agency;

29 or

30 (B) has a reasonable likelihood of materially harming a  
31 consumer residing in this state or a material part of the normal operation of the

1 licensee.

2 (b) To the greatest extent possible and in a form and format prescribed by the  
3 director, the notification to the director under (a) of this section must include the  
4 following information:

5 (1) the date of the cybersecurity event;

6 (2) a description of how nonpublic information was exposed, lost,  
7 stolen, or breached, including the specific roles and responsibilities of third-party  
8 service providers, if any;

9 (3) an explanation of how the cybersecurity event was discovered;

10 (4) whether the lost, stolen, or breached nonpublic information has  
11 been recovered and, if so, how the nonpublic information was recovered;

12 (5) the identity of the source of the cybersecurity event;

13 (6) whether the licensee has filed a police report, or has notified a  
14 regulatory, government, or law enforcement agency about the cybersecurity event and,  
15 if so, the time and date that the licensee notified the agency;

16 (7) a description of the specific types of information acquired without  
17 authorization, such as medical information, financial information, or information  
18 allowing identification of the consumer;

19 (8) the period during which the information system was compromised  
20 by the cybersecurity event;

21 (9) the number of total consumers in this state affected by the  
22 cybersecurity event; the licensee shall provide the licensee's best estimate in the  
23 licensee's initial notification to the director under (a) of this section, and shall update  
24 the estimate with each subsequent notification to the director under (c) of this section;

25 (10) the results of an internal review identifying a lapse in either the  
26 licensee's automated controls or internal procedures or confirming that the licensee  
27 followed all automated controls or internal procedures;

28 (11) a description of efforts the licensee is taking or has taken to  
29 remediate the situation that permitted the cybersecurity event to occur;

30 (12) a copy of the licensee's privacy policy and a statement outlining  
31 the steps the licensee will take to investigate and notify consumers affected by the

1 cybersecurity event; and

2 (13) the name of a contact person who is familiar with the  
3 cybersecurity event and authorized to act on behalf of the licensee.

4 (c) After a licensee provides notice of a cybersecurity event to the director  
5 under (a) of this section, the licensee shall, in a form, format, and frequency prescribed  
6 by the director, update and supplement the information provided under (b) of this  
7 section.

8 (d) In addition to the requirements of this section, a licensee shall comply with  
9 all applicable provisions of AS 45.48 (Alaska Personal Information Protection Act). If  
10 a licensee is required to notify the director of a cybersecurity event under (a) of this  
11 section and is also required to provide notice under AS 45.48, the licensee shall  
12 provide to the director a copy of the notice sent to consumers under AS 45.48.

13 (e) Unless a third-party service provider of a licensee notifies the director, if  
14 the licensee becomes aware of a cybersecurity event that affects an information system  
15 maintained by the third-party service provider, the licensee shall comply with the  
16 requirements of this section to the greatest extent possible. For purposes of this  
17 subsection, the time prescribed in (a) of this section begins the day after the third-party  
18 service provider notifies the licensee of the cybersecurity event or the day after the  
19 date the licensee has actual knowledge of the cybersecurity event, whichever is earlier.

20 (f) A licensee acting as an assuming insurer that determines that a  
21 cybersecurity event has occurred shall, not later than three business days after the  
22 determination, notify the licensee's affected ceding insurers and the insurance  
23 supervisory official of the licensee's state of domicile if

24 (1) the cybersecurity event involves nonpublic information and the  
25 nonpublic information is information used by or in the possession or control of the  
26 licensee acting as an assuming insurer; and

27 (2) the licensee does not have a direct contractual relationship with a  
28 consumer affected by the cybersecurity event.

29 (g) A licensee acting as an assuming insurer that receives notification from the  
30 licensee's third-party service provider that a cybersecurity event has occurred shall, not  
31 later than three business days after receiving notification, notify the licensee's affected

1 ceding insurers and the insurance supervisory official of the licensee's state of  
2 domicile if the cybersecurity event involves nonpublic information and the nonpublic  
3 information is in the possession or control of the third-party service provider.

4 (h) Except as provided in (f) and (g) of this section, a licensee acting as an  
5 assuming insurer does not have other notice obligations relating to a cybersecurity  
6 event under this section.

7 (i) A licensee that is an insurer and that becomes aware that a cybersecurity  
8 event involving nonpublic information has occurred shall, as soon as possible and in a  
9 form and format prescribed by the director, notify each independent insurance  
10 producer of record of a consumer affected by the cybersecurity event if

11 (1) the nonpublic information is in the possession or control of the  
12 licensee or the licensee's third-party service provider;

13 (2) the consumer accessed the insurer's services through the producer;  
14 and

15 (3) the insurer has the current producer of record information for the  
16 consumer.

17 (j) An insurer shall notify an insurance producer of a cybersecurity event  
18 involving nonpublic information, not later than the date the notice is provided to the  
19 affected consumers, if

20 (1) the nonpublic information is in the possession or control of a  
21 licensee that is an insurer or the licensee's third-party service provider;

22 (2) the consumer accessed the insurer's services through an insurance  
23 producer; and

24 (3) the insurer is required to notify affected consumers under  
25 AS 21.23.240 - 21.23.399 or AS 45.48.

26 (k) An insurer is exempt from notifying an insurance producer under (j) of this  
27 section if

28 (1) the producer is not authorized by law or contract to sell, solicit, or  
29 negotiate on behalf of the insurer; or

30 (2) the insurer does not have the current producer information for an  
31 affected consumer.

1           **Sec. 21.23.290. Confidentiality.** (a) Any document, material, or information in  
2 the possession or control of the division that is provided by a licensee or an employee  
3 or agent acting on behalf of a licensee under AS 21.23.260(f) or 21.23.280(b)(2) - (5),  
4 (8), (10), or (11) or that is obtained by the director in an investigation or examination  
5 under AS 21.23.310

6                           (1) is confidential and privileged;

7                           (2) is not subject to inspection and copying under AS 40.25.110 -  
8 40.25.220;

9                           (3) may not be obtained by subpoena or discovery; and

10                          (4) is not admissible in evidence in a private civil action.

11           (b) The director may use a document, material, or information described in (a)  
12 of this section in a regulatory or legal proceeding brought in the performance of the  
13 duties of the director under this title.

14           (c) The director or an individual acting under the authority of the director who  
15 receives a document, material, or information described in (a) of this section may not  
16 testify about the document, material, or information in a private civil action.

17           (d) In the performance of duties under AS 21.23.240 - 21.23.399, the director

18                           (1) may disclose a document, material, or information, including a  
19 document, material, or information that is confidential and privileged or subject to (a)  
20 of this section, to state, federal, and international regulatory or law enforcement  
21 agencies, or to the National Association of Insurance Commissioners and its affiliates  
22 or subsidiaries, if the recipient agrees in writing to maintain the confidentiality and  
23 privileged status of the document, material, or information;

24                           (2) may receive a document, material, or information, including a  
25 document, material, or information that is confidential and privileged, from the  
26 National Association of Insurance Commissioners and its affiliates or subsidiaries, and  
27 from state, federal, and international regulatory or law enforcement agencies; the  
28 director shall maintain as confidential or privileged the document, material, or  
29 information if the entity that provided the director with the document, material, or  
30 information requests the director to do so or gives notice to the director that the  
31 document, material, or information is confidential or privileged under the law of the

1 jurisdiction supplying it;

2 (3) may disclose a document, material, or information that is subject to  
3 (a) of this section with a third-party service provider if the third-party service provider  
4 agrees in writing to maintain the confidentiality and privileged status of the document,  
5 material, or information; and

6 (4) may enter into agreements consistent with this section governing  
7 the sharing and use of a document, material, or information that is confidential or  
8 privileged or subject to (a) of this section.

9 (e) A person does not waive a claim of privilege or confidentiality that the  
10 person possesses by providing a document, material, or information to the director  
11 under AS 21.23.240 - 21.23.399 or by the disclosure, receipt, or sharing of a  
12 document, material, or information under (d) of this section.

13 **Sec. 21.23.300. Applicability.** (a) AS 21.23.250 and 21.23.260 do not apply to

14 (1) a licensee, including an independent contractor, with fewer than 10  
15 employees;

16 (2) a licensee if the licensee is an employee, agent, representative, or  
17 designee of another licensee covered by an information security program.

18 (b) AS 21.23.240 - 21.23.399 do not apply to a licensee subject to the Health  
19 Insurance Portability and Accountability Act of 1996 (P.L. 104-191) if the licensee

20 (1) has established and maintains an information security program  
21 under statutes, regulations, procedures, or guidelines established under the Health  
22 Insurance Portability and Accountability Act of 1996 (P.L. 104-191);

23 (2) is in compliance with the statutes, regulations, procedures, and  
24 guidelines established under the Health Insurance Portability and Accountability Act  
25 of 1996 (P.L. 104-191); and

26 (3) submits to the director a written statement certifying that the  
27 licensee is in compliance with the statutes, regulations, procedures, and guidelines  
28 established under the Health Insurance Portability and Accountability Act of 1996  
29 (P.L. 104-191).

30 (c) If a licensee no longer qualifies for an exception to the applicability of  
31 AS 21.23.240 - 21.23.399 under this section, the licensee shall comply with

1 AS 21.23.240 - 21.23.399 within 180 days after the licensee no longer qualifies for the  
2 exception.

3 **Sec. 21.23.310. Enforcement; penalties.** (a) In addition to the director's power  
4 to examine or investigate under AS 21.06.120, the director may examine and  
5 investigate the affairs of a licensee to determine whether the licensee is or has been in  
6 violation of AS 21.23.240 - 21.23.399. The director shall conduct an examination or  
7 investigation under this section following the same procedures applicable to an  
8 examination or investigation under AS 21.06.120. The director may take necessary or  
9 appropriate action to enforce AS 21.23.240 - 21.23.399.

10 (b) In addition to any other penalty provided by law, a person who violates  
11 AS 21.23.240 - 21.23.399 is subject to the penalties provided under AS 21.27.440.

12 **Sec. 21.23.399. Definitions.** In AS 21.23.240 - 21.23.399,

13 (1) "consumer" means an individual who is a resident of the state and  
14 whose nonpublic information is in a licensee's possession or control;

15 (2) "cybersecurity event"

16 (A) means an event resulting in unauthorized access to or  
17 disruption or misuse of an information system or information stored on the  
18 information system;

19 (B) does not include

20 (i) the unauthorized acquisition of encrypted nonpublic  
21 information if the encryption's process or key is not also acquired,  
22 released, or used without authorization; or

23 (ii) an event in which the licensee has determined that  
24 nonpublic information accessed by an unauthorized person has not been  
25 used or released and has been returned or destroyed;

26 (3) "encrypt" means transforming of data into a form that results in a  
27 low probability of assigning meaning without the use of a protective process or key;

28 (4) "information security program" means the administrative,  
29 technical, and physical safeguards that a licensee uses to access, collect, distribute,  
30 process, protect, store, use, transmit, dispose of, or otherwise handle nonpublic  
31 information;



1 (5) "information system" means

2 (A) a discrete set of electronic information resources organized  
3 for the collection, processing, maintenance, use, sharing, dissemination, or  
4 disposition of electronic information; or

5 (B) a specialized system that may include an industrial or  
6 process control system, a telephone switching and private branch exchange  
7 system, or an environmental control system;

8 (6) "licensee"

9 (A) means a person licensed, authorized to operate, or  
10 registered, or required to be licensed, authorized, or registered, under this title;

11 (B) does not include a purchasing group or a risk retention  
12 group chartered and licensed in a state other than this state or a licensee that is  
13 acting as an assuming insurer that is domiciled in another state or jurisdiction;

14 (7) "nonpublic information" means electronic information that is not  
15 publicly available information and that is

16 (A) business-related information of a licensee, the tampering  
17 with which, or unauthorized disclosure, access, or use of which, would cause a  
18 material adverse effect to the business, operations, or security of the licensee;

19 (B) information concerning a consumer that, because of a  
20 name, number, personal mark, or other identifier, can be used to identify the  
21 consumer in combination with one or more of the following data elements:

22 (i) a social security number;

23 (ii) a driver's license number or identification card  
24 number;

25 (iii) a financial account, credit card, or debit card  
26 number;

27 (iv) a security code, access code, or password that  
28 would permit access to a consumer's financial account; or

29 (v) a biometric record; or

30 (C) information or data, except age or gender, in any form  
31 created by or derived from a health care provider or a consumer that can be

1 used to identify a particular consumer and relates to

2 (i) the past, present, or future physical, mental, or  
3 behavioral health or condition of a consumer or a member of the  
4 consumer's family;

5 (ii) the provision of health care to a consumer; or

6 (iii) payment for the provision of health care to a  
7 consumer;

8 (8) "person" means an individual or a nongovernmental entity;

9 (9) "publicly available information" means information that a licensee  
10 has determined is made available to the general public from

11 (A) a federal, state, or local government record;

12 (B) a widely distributed media; or

13 (C) a disclosure to the general public that is required under  
14 federal, state, or local law;

15 (10) "third-party service provider" means a person that is not a licensee  
16 that, through a contract with a licensee, is permitted access to and maintains,  
17 processes, or stores nonpublic information through its provision of services to the  
18 licensee.

19 \* **Sec. 2.** AS 21.42.375(e) is amended to read:

20 (e) In this section,

21 **(1) "diagnostic breast examination" means an examination of the**  
22 **breast using contrast-enhanced mammography, diagnostic mammography,**  
23 **breast magnetic resonance imaging, breast ultrasound, or other equipment**  
24 **dedicated specifically for mammography conducted to evaluate an abnormality**

25 **(A) detected or suspected in a screening examination for**  
26 **breast cancer; or**

27 **(B) detected by another means of examination;**

28 **(2)** "low-dose mammography screening" and "mammogram" mean the  
29 X-ray examination of the breast using equipment dedicated specifically for  
30 mammography, including the X-ray tube, filter, compression device, screens, films,  
31 and cassettes, with an average radiation exposure delivery of less than one rad mid-

1 breast, with two views for each breast;

2 **(3) "supplemental breast examination" means an examination of**  
3 **the breast using contrast-enhanced mammography, diagnostic mammography,**  
4 **breast magnetic resonance imaging, breast ultrasound, or other equipment**  
5 **dedicated specifically for mammography conducted based on**

6 **(A) the insured's personal or family medical history of**  
7 **breast cancer; or**

8 **(B) other factors that may increase the insured's risk of**  
9 **breast cancer.**

10 \* **Sec. 3.** AS 21.42.375 is amended by adding a new subsection to read:

11 (f) Except as necessary to qualify a plan as a high deductible health plan  
12 eligible for a health savings account tax deduction under 26 U.S.C. 223 (Internal  
13 Revenue Code), a health care insurer that offers, issues, delivers, or renews a health  
14 care insurance plan in the individual or group market in the state that provides  
15 coverage for mammography screening, diagnostic breast examinations, and  
16 supplemental breast examinations may not impose cost sharing, a deductible,  
17 coinsurance, a copayment obligation, or another similar out-of-pocket expense on an  
18 insured for coverage of a low-dose mammography screening, diagnostic breast  
19 examination, or supplemental breast examination.

20 \* **Sec. 4.** The uncodified law of the State of Alaska is amended by adding a new section to  
21 read:

22 **INDIRECT COURT RULE AMENDMENTS.** (a) AS 21.23.290(a)(3), enacted by sec.  
23 1 of this Act, has the effect of changing Rule 26, Alaska Rules of Civil Procedure, by  
24 prohibiting discovery of evidence in the possession or control of the division of insurance that  
25 is provided by a licensee or an employee or agent acting on behalf of a licensee under  
26 AS 21.23.260(f) or 21.23.280(b)(2) - (5), (8), (10), or (11) or that is obtained by the director  
27 in an investigation or examination under AS 21.23.310.

28 (b) AS 21.23.290(a)(4) and (c), enacted by sec. 1 of this Act, have the effect of  
29 changing Rules 402 and 501, Alaska Rules of Evidence, by

30 (1) creating a new privilege that would prevent the director of the division of  
31 insurance, or an individual acting under the authority of the director, from being permitted or

1 compelled to testify about confidential or privileged documents, materials, or information in a  
2 private civil action; and

3 (2) precluding admissibility of evidence in a private action of documents,  
4 materials, or other information in the possession or control of the division of insurance that is  
5 provided by a licensee or an employee or agent acting on behalf of a licensee under  
6 AS 21.23.260(f) or 21.23.280(b)(2) - (5), (8), (10), or (11) or that is obtained by the director  
7 in an investigation or examination under AS 21.23.310.

8 \* **Sec. 5.** The uncodified law of the State of Alaska is amended by adding a new section to  
9 read:

10 APPLICABILITY. AS 21.42.375(e), as amended by sec. 2 of this Act, and  
11 AS 21.42.375(f), added by sec. 3 of this Act, apply to an insurance policy or contract issued,  
12 delivered, or renewed on or after the effective date of secs. 2 and 3 of this Act.

13 \* **Sec. 6.** The uncodified law of the State of Alaska is amended by adding a new section to  
14 read:

15 TRANSITION: REGULATIONS. The director of the division of insurance may adopt  
16 regulations necessary to implement this Act. The regulations take effect under AS 44.62  
17 (Administrative Procedure Act), but not before the effective date of the law implemented by  
18 the regulation.

19 \* **Sec. 7.** The uncodified law of the State of Alaska is amended by adding a new section to  
20 read:

21 CONDITIONAL EFFECT. AS 21.23.290(a)(3) and (4) and (c), enacted by sec. 1 of  
22 this Act, take effect only if sec. 4 of this Act receives the two-thirds majority vote of each  
23 house required by art. IV, sec. 15, Constitution of the State of Alaska.

24 \* **Sec. 8.** Section 6 of this Act takes effect immediately under AS 01.10.070(c).

25 \* **Sec. 9.** If AS 21.23.290(a)(3) and (4) and (c), enacted by sec. 1 of this Act, take effect,  
26 they take effect January 1, 2025.

27 \* **Sec. 10.** AS 21.23.250 and 21.23.260(a), (b), (c)(1) - (6) and (9) - (11), and (d) - (g),  
28 enacted by sec. 1 of this Act, take effect January 1, 2026.

29 \* **Sec. 11.** AS 21.23.260(c)(7) and (8), enacted by sec. 1 of this Act, take effect January 1,  
30 2027.

31 \* **Sec. 12.** Except as provided in secs. 8 - 11 of this Act, this Act takes effect January 1,

1 2025.