House of Representatives

General Assembly

File No. 338

January Session, 2021

Substitute House Bill No. 6391

House of Representatives, April 8, 2021

The Committee on Insurance and Real Estate reported through REP. WOOD, K. of the 29th Dist., Chairperson of the Committee on the part of the House, that the substitute bill ought to pass.

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

Be it enacted by the Senate and House of Representatives in General Assembly convened:

Section 1. Subsections (b) and (c) of section 19a-7p of the general statutes are repealed and the following is substituted in lieu thereof (*Effective July 1, 2021*):

(b) (1) As used in this section: (A) "Health insurance" means health insurance of the types specified in subdivisions (1), (2), (4), (11) and (12) of section 38a-469; and (B) "health care center" has the same meaning as provided in section 38a-175.

(2) Each domestic insurer or domestic health care center doing health insurance business in this state shall annually pay to the Insurance Commissioner, for deposit in the Insurance Fund established under section 38a-52a, a public health fee assessed by the Insurance Commissioner pursuant to this section.

(3) (A) Not later than September first, annually, each such insurer or health care center shall report to the Insurance Commissioner, in the form and manner prescribed by **[**said**]** the commissioner, the number of insured or enrolled lives in this state as of May first immediately preceding the date for which such insurer or health care center is providing health insurance that provides coverage of the types specified in subdivisions (1), (2), (4), (11) and (12) of section 38a-469. Such number shall not include lives enrolled in Medicare, any medical assistance program administered by the Department of Social Services, workers' compensation insurance or Medicare Part C plans. The commissioner may require each such insurer or health care center or any other person to submit to the commissioner any records that are in such insurer's, health care center's or other person's possession if such records were used to prepare such insurer's or health care center's annual report submitted pursuant to this subparagraph.

(B) Each such insurer or health care center that fails to timely submit an annual report pursuant to subparagraph (A) of this subdivision shall pay to the Insurance Commissioner, in the form and manner prescribed by the commissioner, a late filing fee of one hundred dollars per day for each day from the date that the annual report was due.

(C) If the Insurance Commissioner determines that there is a discrepancy, other than a good faith discrepancy, between the number of insured or enrolled lives that the insurer or health care center reported to the commissioner pursuant to subparagraph (A) of this subdivision and the number of such lives that the insurer or health care center should have reported to the commissioner pursuant to said subparagraph (A), the insurer or health care center shall be liable for a civil penalty of not more than fifteen thousand dollars.

(c) Not later than November first, annually, the Insurance Commissioner shall determine the fee to be assessed for the current fiscal year against each such insurer and health care center. Such fee shall be calculated by multiplying the number of lives reported to said commissioner pursuant to subparagraph (A) of subdivision (3) of

subsection (b) of this section by a factor, determined annually by said commissioner as set forth in this subsection, to fully fund the aggregate amount determined under subsection (a) of this section. The Insurance Commissioner shall determine the factor by dividing the aggregate amount by the total number of lives reported to said commissioner pursuant to subparagraph (A) of subdivision (3) of subsection (b) of this section.

Sec. 2. Section 38a-12 of the general statutes is repealed and the following is substituted in lieu thereof (*Effective from passage*):

[(a)**]** The commissioner shall, annually, submit to the Governor a report of the commissioner's official acts and of the condition of all insurance companies doing business in this state, with a condensed statement of their reports made to the commissioner or accepted by the commissioner, together with an abstract of all accounts rendered to any court by any receiver of a domestic insurance company, a statement of the fees received by the commissioner and paid by the commissioner to the Treasurer and such other facts as are required by law.

[(b) On or before January fifteenth annually, the commissioner shall submit to the joint standing committee of the General Assembly having cognizance of matters relating to insurance a report, in accordance with the provisions of section 11-4a, detailing all the information the commissioner received during the past year pursuant to sections 29-311, 31-290d, 38a-356 and 53-445.**]**

Sec. 3. Subsections (b) to (g), inclusive, of section 38a-38 of the general statutes are repealed and the following is substituted in lieu thereof (*Effective from passage*):

(b) Definitions. For the purposes of this section:

(1) "Authorized individual" means an individual who is known to, and screened by, a licensee, and who is determined to be necessary and appropriate to have access to the nonpublic information that is held by the licensee and on such licensee's information systems.

(2) "Consumer" means an individual, including, but not limited to, an applicant, beneficiary, certificate holder, claimant, insured or policyholder, who is a resident of this state and whose nonpublic information is in a licensee's possession, custody or control.

(3) "Cybersecurity event" means an event resulting in any unauthorized access to, or disruption or misuse of, an information system or the nonpublic information stored thereon, except if: (A) The event involves the unauthorized acquisition of encrypted nonpublic information if the encryption process for such information or encryption key to such information is not acquired, released or used without authorization; or (B) the event involves access of nonpublic information by an unauthorized person and the licensee determines that such information has not been used or released and has been returned or destroyed.

(4) "Encryption" means the transformation of data or information into a form that results in a low probability of assigning meaning to such data or information without the use of a protective process or key.

(5) "Information security program" means the administrative, technical and physical safeguards that a licensee uses to access, collect, distribute, process, protect, store, use, transmit, dispose of or otherwise handle nonpublic information.

(6) "Information system" means a discrete set of electronic information resources organized for the collection, processing, maintenance, use, sharing, dissemination or disposition of nonpublic electronic data or information, as well as any specialized system such as an industrial or process controls system, telephone switching and private branch exchange system, and environmental control system.

(7) "Licensee" means any person licensed, authorized to operate or registered, or required to be licensed, authorized to operate or registered, pursuant to the insurance laws of this state, **[**except for**]** including, but not limited to, a fraternal benefit society, an interlocal risk management agency formed pursuant to chapter 113a or an employers'

mutual association authorized under part C of chapter 568, but not including a purchasing group or [a] risk retention group chartered and licensed in another state, [or] a [licensee that is] person acting as an assuming insurer and domiciled in another state or jurisdiction or a commissioner of the Superior Court acting as a title agent, as defined in section 38a-402.

(8) "Multifactor authentication" means authentication through verification of at least two of the following types of authentication factors: (A) A knowledge factor, including, but not limited to, a password; (B) a possession factor, including, but not limited to, a token or text message on a mobile phone; or (C) an inheritance factor, including, but not limited to, a biometric characteristic.

(9) "Nonpublic information" means electronic data and information, other than publicly available information and [information concerning] a consumer's age or gender, that: (A) Concerns the business of a licensee and that, if accessed, disclosed, tampered with or used without authorization from the licensee, would have a material adverse impact on the business, operations or security of such licensee; (B) concerns a consumer and that, because such data or information contains a name, number, personal mark or other identifier, can be used to identify such consumer in combination with: (i) A Social Security number; (ii) a driver's license number or nondriver identification card number; (iii) an account, credit or debit card number; (iv) an access or security code, or a password, that would permit access to the consumer's financial account; or (v) a biometric record; or (C) is in a form or medium created by, or derived from, a health care provider or consumer and concerns: (i) The past, present or future physical, mental or behavioral health or condition of a consumer or a member of a consumer's family; (ii) the provision of health care to a consumer; or (iii) payment for the provision of health care to a consumer.

(10) "Person" means any individual or any nongovernmental entity, including, but not limited to, any nongovernmental partnership, corporation, branch, agency or association.

(11) "Publicly available information" means data or information that: (A) (i) Must be disclosed to the general public pursuant to applicable law; or (ii) may be made available to the general public from government records or widely distributed media; and (B) a licensee reasonably believes, after investigation: (i) Is of a type that is available to the general public; and (ii) the consumer has not directed to be withheld from the general public, if the consumer may direct that such data or information be withheld from the general public pursuant to applicable law.

(12) "Risk assessment" means the risk assessment that each licensee is required to conduct pursuant to subdivision (3) of subsection (c) of this section.

(13) "Third-party service provider" means a person, other than a licensee, that: (A) Contracts with a licensee to maintain, process or store nonpublic information; or (B) is otherwise permitted to access nonpublic information through the person's provision of services to a licensee.

(c) Information Security Program. (1) Implementation of an information security program. Except as provided in subdivision (10) of this subsection, each licensee shall, not later than October 1, **[**2020**]** 2021, develop, implement and maintain a comprehensive written information security program that is based on the licensee's risk assessment and contains the administrative, technical and physical safeguards for the protection of nonpublic information and such licensee's information systems. Each information security program shall be commensurate with the size and complexity of the licensee, the nature and scope of the licensee's activities, including, but not limited to, such licensee's use of third-party service providers, and the sensitivity of the nonpublic information used by such licensee or in such licensee's possession, custody or control.

(2) Objectives of Information Security Program. Except as provided in subdivision (10) of this subsection, each information security program developed, implemented and maintained by a licensee pursuant to subdivision (1) of this subsection shall:

(A) Be designed to:

(i) Protect the security and confidentiality of the nonpublic information and the security of the information system;

(ii) Protect against all threats and hazards to the security or integrity of nonpublic information and the information system; and

(iii) Protect against unauthorized access to, or use of, nonpublic information and minimize the likelihood of harm to any consumer; and

(B) Define, and periodically reevaluate, a schedule for retention of nonpublic information and a mechanism for the destruction of such information when such information no longer is needed.

(3) Risk Assessment. Except as provided in subdivision (10) of this subsection, each licensee shall:

(A) Designate one or more employees, an affiliate or an outside vendor designated to act on behalf of such licensee as the person responsible for such licensee's information security program;

(B) Identify reasonably foreseeable internal or external threats that could result in unauthorized access, transmission, disclosure, misuse, alteration or destruction of nonpublic information, including, but not limited to, the security of information systems that are, and nonpublic information that is, accessible to, or held by, third-party service providers;

(C) Assess the likelihood and potential damage of the threats identified pursuant to subparagraph (B) of this subdivision, taking into consideration the sensitivity of the nonpublic information;

(D) Assess the sufficiency of policies, procedures, information systems and other safeguards in place to manage the threats identified pursuant to subparagraph (B) of this subdivision by considering such threats in the following areas of such licensee's operations:

(i) Employee training and management;

(ii) Information systems, including, but not limited to, network and software design, as well as information classification, governance, processing, storage, transmission and disposal; and

(iii) Detection, prevention and response to attacks, intrusions or other systems failures;

(E) Implement information safeguards to manage the threats identified in such licensee's ongoing assessment; and

(F) Not less than annually, assess the effectiveness of such licensee's safeguards' key controls, systems and procedures.

(4) Risk Management. Except as provided in subdivision (10) of this subsection, each licensee shall, based on such licensee's risk assessment:

(A) Design such licensee's information security program to mitigate the identified risks, commensurate with the size and complexity of such licensee's activities, including, but not limited to, such licensee's use of third-party service providers, and the sensitivity of the nonpublic information used by such licensee or in such licensee's possession, custody or control.

(B) Determine which of the following security measures are appropriate and, if such measures are appropriate, implement such measures:

(i) Placement of access controls on such licensee's information systems, including, but not limited to, controls to authenticate and restrict access only to authorized individuals to protect against the unauthorized acquisition of nonpublic information;

(ii) Identification and management of the data, personnel, devices, systems and facilities that enable such licensee to achieve such licensee's business purposes in accordance with their relative importance to such licensee's business objectives and risk strategy;

(iii) Restriction of access to physical locations containing nonpublic

information only to authorized individuals;

(iv) Protection, by encryption or other appropriate means, of all nonpublic information while such information is transmitted over an external network or stored on a laptop computer or other portable computing or storage device or medium;

(v) Adoption of secure development practices for in-house developed applications utilized by such licensee and procedures for evaluating, assessing or testing the security of externally developed applications utilized by such licensee;

(vi) Modification of such licensee's information system in accordance with such licensee's information security program;

(vii) Utilization of effective controls, which may include multifactor authentication procedures for any individual accessing nonpublic information;

(viii) Regular testing and monitoring of systems and procedures to detect actual and attempted attacks on, or intrusions into, information systems;

(ix) Inclusion of audit trails within the information security program that are designed to detect and respond to cybersecurity events, and designed to reconstruct material financial transactions sufficient to support the normal operations and obligations of the licensee;

(x) Implementation of measures to protect against the destruction, loss or damage of nonpublic information due to environmental hazards, including, but not limited to, fire and water, or other catastrophes or technological failures; and

(xi) Development, implementation and maintenance of procedures for the secure disposal of nonpublic information in any format.

(C) Include cybersecurity risks in such licensee's enterprise risk management process.

(D) Stay informed regarding emerging threats or vulnerabilities and utilize reasonable security measures when sharing information relative to the character of the sharing and the type of information shared.

(E) Provide such licensee's personnel with cybersecurity awareness training that is updated as necessary to reflect risks identified by such licensee in such licensee's risk assessment.

(5) Oversight by Board of Directors. Except as provided in subdivision (10) of this subsection, if a licensee has a board of directors, the board, or an appropriate committee of such board, shall, at a minimum:

(A) Require the licensee's executive management or **[**its**]** such executive management's delegates to develop, implement and maintain such licensee's information security program.

(B) Require the licensee's executive management or **[**its**]** such executive management's delegates to report, in writing and at least annually, the following information:

(i) The overall status of such licensee's information security program and such licensee's compliance with this section; and

(ii) Material matters related to such licensee's information security program, addressing issues such as risk assessment, risk management and control decisions, third-party service provider arrangements, results of testing, cybersecurity events or violations and management's responses thereto, and recommendations for changes in such information security program.

(C) If a licensee's executive management delegates any of **[**its**]** such executive management's responsibilities under subparagraph (A) or (B) of this subdivision, **[**it**]** such executive management shall oversee the development, implementation and maintenance of the licensee's information security program prepared by the delegate or delegates, and shall receive a report from such delegate or delegates that satisfies the requirements established in subparagraph (B) of this subdivision.

(6) Oversight of Third-Party Service Provider Arrangements. Except as provided in subdivision (10) of this subsection:

(A) Each licensee shall exercise due diligence in selecting such licensee's third-party service providers; and

(B) Not later than October 1, **[**2021**]** 2022, each licensee shall require each of such licensee's third-party service providers to implement appropriate administrative, technical and physical measures to protect and secure the information systems that are, and nonpublic information that is, accessible to, or held by, such licensee's third-party service providers.

(7) Program Adjustments. Except as provided in subdivision (10) of this subsection, each licensee shall monitor, evaluate and adjust, as appropriate, such licensee's information security program consistent with any relevant changes in technology, the sensitivity of **[**such licensee's**]** the nonpublic information in such licensee's possession, custody or control, internal or external threats to such information and such licensee's own changing business arrangements, including, but not limited to, changes stemming from mergers and acquisitions, alliances and joint ventures, outsourcing arrangements and changes to information systems.

(8) Incident Response Plan. (A) Except as provided in subdivision (10) of this subsection, each licensee shall, as part of such licensee's information security program, establish a written incident response plan that is designed to promptly respond to, and recover from, any cybersecurity event that compromises the confidentiality, integrity or availability of nonpublic information that is in such licensee's possession, custody or control, such licensee's information systems or the continuing functionality of any aspect of such licensee's business or operations.

(B) Each incident response plan shall address the following areas:

(i) The internal process for responding to a cybersecurity event;

(ii) The goals of such incident response plan;

(iii) The definition of clear roles, responsibilities and levels of decision-making authority;

(iv) External and internal communications;

(v) Information sharing;

(vi) Identification of requirements for the remediation of any identified weaknesses in information systems and associated controls;

(vii) Documentation and reporting regarding cybersecurity events and related incident response activities; and

(viii) Evaluation and revision, as necessary, of such incident response plan following each cybersecurity event.

(9) Annual Certification to Commissioner of Domiciliary State. Except as provided in subdivision (10) of this subsection, each insurer, health care center or fraternal benefit society domiciled in this state shall submit to the Insurance Commissioner a written statement, not later than **[**February**]** April fifteenth, annually, certifying that such insurer, health care center or fraternal benefit society is in compliance with the requirements set forth in this subsection. **[**Each insurer shall**]** A domestic insurer, health care center or fraternal benefit society that is a member of an insurance holding company system, as defined in section 38a-129, may submit one statement to the Insurance Commissioner on behalf of other domestic insurers, health care centers or fraternal benefit societies that are members of the same insurance holding company system, not later than April fifteenth, annually, certifying that such domestic members of the insurance holding company system are in compliance with the requirements set forth in this subsection. Each insurer, health care center or fraternal benefit society shall, either directly or through an affiliate, maintain, for examination by the Insurance Department, all records, schedules and data supporting each statement that such insurer, health care center or fraternal benefit society, or a member of an insurance holding company system acting on behalf of such insurer,

health care center or fraternal benefit society, submits to the commissioner for a period of five years. To the extent an insurer, health care center or fraternal benefit society has identified areas, systems or processes that require material improvement, updating or redesign, the insurer, health care center or fraternal benefit society shall, either directly or through an affiliate, document such identification and the remedial efforts planned and underway to address such areas, systems or processes. Such documentation must be available for inspection by the commissioner.

(10) Exceptions. (A) The following exceptions shall apply to this subsection:

(i) (I) During the period beginning on October 1, **[**2020**]** 2021, and ending on September 30, **[**2021**]** 2022, each licensee with fewer than twenty employees, which, for the purposes of this subclause, includes independent contractors having access to the nonpublic information used by such licensee or in such licensee's possession, custody or control, shall be exempt from this subsection; and

(II) On and after October 1, **[**2021**]** 2022, each licensee with fewer than ten employees, which, for the purposes of this subclause, includes independent contractors having access to the nonpublic information used by such licensee or in such licensee's possession, custody or control, shall be exempt from this subsection;

(ii) Each licensee that is subject to the Health Insurance Portability and Accountability Act of 1996, P.L. 104-191, as amended from time to time, and has established and maintains an information security program pursuant to said act and the rules, regulations, procedures or guidelines established thereunder, shall be deemed to have satisfied the requirements of this subsection, provided such licensee is in compliance therewith and submits to the Insurance Commissioner, not later than April fifteenth, annually, a written statement certifying such licensee's compliance therewith;

(iii) Each employee, agent, representative or designee of a licensee,

who is also a licensee, shall be exempt from the provisions of this subsection and need not develop its own information security program to the extent that such employee, agent representative or designee is covered by the other licensee's information security program; and

(iv) Each licensee that has established and maintains an information security program in compliance with **[**the statutes, rules and regulations of a jurisdiction approved by the commissioner pursuant to regulations adopted pursuant to subsection (i) of this section**]** Part 500 of Chapter I of Title 23 of the New York Codes, Rules and Regulations, as amended from time to time, shall be deemed to have satisfied the provisions of this subsection, provided such licensee is in compliance therewith and submits to the commissioner, not later than **[**February**]** April fifteenth, annually, a written statement certifying such licensee's compliance therewith.

(B) In the event that a licensee ceases to qualify for an exception under this subdivision, the licensee shall have one hundred eighty days to comply with this subsection.

(d) Investigation of a Cybersecurity Event. (1) If a licensee learns that a cybersecurity event has, or may have, occurred, the licensee, or an outside vendor or service provider, or both, designated to act on behalf of such licensee, shall conduct a prompt investigation in accordance with the provisions of this subsection.

(2) During any investigation conducted pursuant to subdivision (1) of this subsection, the licensee or the outside vendor or service provider, or both, shall, at a minimum and to the extent possible:

(A) Determine whether the cybersecurity event occurred; and

(B) If the cybersecurity event occurred:

(i) Assess the nature and scope of such cybersecurity event;

(ii) Identify the nonpublic information, if any, that may have been involved in such cybersecurity event; and

(iii) Perform or oversee reasonable measures to restore the security of the information systems compromised in such cybersecurity event in order to prevent further unauthorized acquisition, release or use of nonpublic information that is in the licensee's possession, custody or control.

(3) If a licensee learns that a cybersecurity event has, or may have, occurred in a system maintained by a third-party service provider, the licensee shall complete the steps listed in subdivision (2) of this subsection or confirm and document that the third-party service provider has completed such steps.

(4) Each licensee that is subject to the provisions of this subsection shall maintain records concerning each cybersecurity event for a period of at least five years from the date of such cybersecurity event, and shall produce such records to the Insurance Commissioner upon demand by the commissioner.

(e) Notification of a Cybersecurity Event. (1) Notification to the Commissioner. Each licensee shall notify the Insurance Commissioner that a cybersecurity event has occurred, as promptly as possible but in no event later than three business days after the date **[**of the**]** on which such licensee first determines that a cybersecurity event has occurred, if:

(A) Such licensee is an insurer and this state is the insurer's state of domicile, or the licensee is an insurance producer, as defined in section 38a-702a, and this state is the insurance producer's home state, as defined in section 38a-702a, **[**;**]** and it is reasonably likely that the cybersecurity event will materially harm:

(i) A consumer residing in this state; or

(ii) A material part of such licensee's normal operations; or

(B) The licensee reasonably believes that the nonpublic information involved in the cybersecurity event is of two hundred fifty or more consumers residing in this state and:

(i) State or federal law requires that a notice concerning such cybersecurity event be provided to a government body, self-regulatory agency or another supervisory body; or

(ii) It is reasonably likely that such cybersecurity event will materially harm:

(I) A consumer residing in this state; or

(II) A material part of such licensee's normal operations.

(2) Information to Be Provided to Commissioner. (A) Each licensee that notifies the Insurance Commissioner pursuant to subdivision (1) of this subsection shall provide to the commissioner, in an electronic form prescribed by the commissioner, as much of the following information as possible:

(i) The date of the cybersecurity event;

(ii) A description of how the information was exposed, lost, stolen or breached, including, but not limited to, the specific roles and responsibilities of third-party service providers, if any;

(iii) How, and the date on which, the cybersecurity event was discovered;

(iv) Whether any lost, stolen or breached information has been recovered, and, if so, how such information was recovered;

(v) The identity of the source of the cybersecurity event;

(vi) Whether such licensee has filed a police report or notified any regulatory, government or law enforcement agency, and, if so, when such licensee filed such report or provided such notice;

(vii) A description of the specific types of exposed, lost, stolen or breached information, including, for example, specific types of medical information, financial information or information allowing identification of a consumer;

(viii) The period during which each information system that was compromised by the cybersecurity event was compromised by such cybersecurity event;

(ix) The number of total consumers residing in this state that, within such licensee's knowledge at the time that such licensee discloses such number to the commissioner, are affected by the cybersecurity event;

(x) The results of an internal review identifying any lapse in automated controls or internal procedures, or confirming that all such controls and procedures were followed;

(xi) A description of any efforts being undertaken to remediate the situation that permitted the cybersecurity event to occur;

(xii) A copy of the licensee's privacy policy and a statement outlining the steps the licensee will take to investigate and notify consumers affected by the cybersecurity event; and

(xiii) The name of a contact person who is both familiar with the cybersecurity event and authorized to act for the licensee.

(B) Each licensee that provides information to the Insurance Commissioner pursuant to subparagraph (A) of this subdivision shall have a continuing obligation to update and supplement such information.

(3) Notification to Consumers. Each licensee shall comply with all applicable provisions of section 36a-701b, and provide to the Insurance Commissioner a copy of the notice that such licensee sends to consumers pursuant to said section, if any, if such licensee is required to notify the commissioner pursuant to subdivision (1) of this subsection.

(4) Notice Regarding Cybersecurity Events of Third-Party Service Providers. (A) In the case of a cybersecurity event involving **[**a**]** an information system maintained by a third-party service provider, each licensee affected by the event shall treat such event, if the licensee **[**as**]** is

aware of such event, as such licensee would treat such event under subdivision (1) of this subsection.

(B) The computation of a licensee's deadlines shall begin on the day after a third-party service provider notifies the licensee of the cybersecurity event or such licensee otherwise first **[**becomes aware**]** has actual knowledge of such event, whichever is sooner.

(C) Nothing in this section shall prevent or abrogate an agreement between a licensee and another party to fulfill any of the investigation requirements imposed under subsection (d) of this section or the notice requirements imposed under this subsection.

(5) Notice Regarding Cybersecurity Events of Reinsurers to Insurers. (A) (i) In the case of a cybersecurity event involving nonpublic information that is used by a licensee that is acting as an assuming insurer or in the possession, custody or control of a licensee that is acting as an assuming insurer and that does not have a direct contractual relationship with the affected consumers, the assuming insurer shall notify its affected ceding insurers and the insurance regulatory official of its state of domicile not later than seventy-two hours after such assuming insurer discovered that the cybersecurity event had occurred.

(ii) Each ceding insurer that has a direct contractual relationship with the consumers affected by a cybersecurity event shall fulfill the consumer notification requirements imposed under section 36a-701b and any other notification requirements relating to a cybersecurity event imposed under this section.

(B) (i) In the case of a cybersecurity event involving nonpublic information that is in the possession, custody or control of a third-party service provider of a licensee, when the licensee is acting as an assuming insurer, including an assuming insurer that is domiciled in another state or jurisdiction, the assuming insurer shall notify its affected ceding insurers and the insurance regulatory official of its state of domicile not later than seventy-two hours after such assuming insurer received notice from the third-party service provider disclosing that the

cybersecurity event occurred.

(ii) Ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under section 36a-701b and any other notification requirements relating to a cybersecurity event imposed under this section.

(6) Notice Regarding Cybersecurity Events of Insurers to Producers of Record. If a cybersecurity event involves nonpublic information that is in the possession, custody or control of a licensee that is an insurer, or a third-party service provider for a licensee that is an insurer, and for which a consumer who is affected by the cybersecurity event accessed such licensee's services through an independent insurance producer, such licensee shall notify the producer of record for such consumer of the occurrence of such cybersecurity event in a reasonable manner and not later than the time at which notice is provided to such consumer, provided such licensee has the current producer of record information for such individual consumer.

(f) Power of Commissioner. (1) The Insurance Commissioner shall have power to examine and investigate into the affairs of a licensee to determine whether the licensee is, or has been, engaged in conduct in this state that violates the provisions of this section. The commissioner's power under this subsection is in addition to the commissioner's powers under sections 38a-14 to 38a-16, inclusive. Any such investigation or examination shall be conducted pursuant to said sections, if applicable.

(2) Whenever the Insurance Commissioner has reason to believe that a licensee is, or has been, engaged in conduct in this state that violates the provisions of this section, the commissioner shall issue and serve upon the licensee:

(A) A statement setting forth such violation; and

(B) A notice of a hearing to be held at a time and place fixed in such notice, which time shall not be less than thirty calendar days after the

date of service of such notice.

(3) (A) The licensee shall, at the time and place fixed for the hearing in the notice issued and served upon such licensee pursuant to subdivision (2) of this subsection, have an opportunity to be heard and show cause why an order should not be entered by the Insurance Commissioner:

(i) Enforcing the provisions of this section; or

(ii) Suspending, revoking or refusing to reissue or renew any license, certificate of registration or authorization to operate the Insurance Commissioner has issued, or may issue, to such licensee.

(B) The Insurance Commissioner may, after holding a hearing pursuant to subparagraph (A) of this subdivision, take any action that is necessary or appropriate to enforce the provisions of this section and, in addition to or in lieu of suspending, revoking or refusing to reissue or renew any license, certificate of registration or authorization to operate the commissioner has issued, or may issue, to the licensee, impose on such licensee a civil penalty of not more than fifty thousand dollars for each violation of the provisions of this section. The commissioner may bring a civil action to recover the amount of any civil penalty that the commissioner imposes on a licensee pursuant to this subparagraph.

(g) Confidentiality. (1) (A) Except as provided in subparagraph (B) of this subdivision, documents, materials and other information in the possession, custody or control of the Insurance Department and furnished to the department by a licensee, or an employee or agent of a licensee acting on behalf of the licensee, pursuant to subdivision (9) of subsection (c) of this section or subparagraph (A)(ii), (A)(iii), (A)(iv), (A)(v), (A)(viii), (A)(x) or (A)(xi) of subdivision (2) of subsection (e) of this section, or obtained by the commissioner in an investigation or examination conducted pursuant to subsection (f) of this section, shall be confidential by law, privileged, not subject to disclosure under section 1-210, not subject to subpoena, and not subject to discovery or

admission into evidence in any private civil action.

(B) The Insurance Commissioner is authorized to use all documents, materials and other information in furtherance of any regulatory or legal actions brought as a part of the commissioner's duties.

(2) Neither the Insurance Commissioner nor any person acting under the authority of the commissioner who receives documents or materials that are, or other information that is, subject to the provisions of subdivision (1) of this subsection shall be permitted or required to testify in any private civil action concerning such documents, materials or other information.

(3) The Insurance Commissioner, in **[**order to assist the commissioner in performing**]** furtherance of the commissioner's duties under this section, may:

(A) Share documents, materials and other information, including, but not limited to, confidential and privileged documents, materials and other information subject to subdivision (1) of this subsection, with other state, federal and international regulatory agencies, the National Association of Insurance Commissioners and the affiliates and subsidiaries of said association, the Attorney General and other state, federal or international law enforcement authorities, provided the recipient of such documents, materials or other information agrees, in writing, to maintain the confidentiality and privileged status of such documents, materials or other information;

(B) Receive documents, materials and other information, including, but not limited to, otherwise confidential and privileged documents, materials and other information, from the National Association of Insurance Commissioners and the affiliates and subsidiaries of said association, the Attorney General and other domestic or foreign regulatory or law enforcement officials, provided the commissioner shall maintain as confidential and privileged all documents, materials and other information that the commissioner receives with notice or an understanding that such documents or materials are, or such other

information is, confidential or privileged under the laws of the jurisdiction that is the source of such documents, materials or other information;

(C) Share documents, materials and other information subject to subdivision (1) of this subsection with a third-party consultant or vendor, provided the third-party consultant or vendor agrees, in writing, to maintain the confidentiality and privileged status of such documents, materials and other information; and

(D) Enter into agreements governing the sharing and use of documents, materials and other information, provided such agreements are consistent with the provisions of this subsection.

(4) No waiver of any applicable privilege or claim of confidentiality in a document, material or other information shall occur as a result of any disclosure of the document, material or other information to the Insurance Commissioner pursuant to this section, or as a result of any sharing of such document, material or other information authorized under subdivision (3) of this subsection.

(5) Nothing in this section shall prohibit the Insurance Commissioner from releasing final, adjudicated actions that are open to public inspection pursuant to section 1-210 to a database or other clearinghouse service maintained by the National Association of Insurance Commissioners or the affiliates or subsidiaries of said association.

(6) All documents, materials and other information provided to, and in the possession, custody or control of, the National Association of Insurance Commissioners or a third-party consultant or vendor pursuant to this section shall be confidential by law, privileged, not be subject to disclosure under section 1-210, not subject to subpoena, and not subject to discovery or admission into evidence in any private civil action.

Sec. 4. Subsection (g) of section 38a-48 of the general statutes is repealed and the following is substituted in lieu thereof (*Effective July 1,*

2021):

(g) If the actual expenditures for the fall prevention program established in section 17a-303a are less than the amount allocated, the Commissioner of Aging and Disability Services shall notify the Insurance Commissioner and the Healthcare Advocate. Immediately following the close of the fiscal year, the Insurance Commissioner and the Healthcare Advocate shall recalculate the proposed assessment for each domestic insurance company or other domestic entity in accordance with subsection (c) of this section using the actual expenditures made during the fiscal year by the Insurance Department, the Office of the Healthcare Advocate and the Office of Health Strategy from the Insurance Fund, the actual expenditures made on behalf of the department and the offices from the Capital Equipment Purchase Fund pursuant to section 4a-9, not including such expenditures made on behalf of the Health Systems Planning Unit of the Office of Health Strategy, and the actual expenditures for the fall prevention program. On or before July thirty-first, the Insurance Commissioner and the Healthcare Advocate shall render to each such domestic insurance company and other domestic entity a statement showing the difference between their respective recalculated assessments and the amount they have previously paid. On or before August thirty-first, the Insurance Commissioner and the Healthcare Advocate, after receiving any objections to such statements, shall make such adjustments which in their opinion may be indicated, and shall render an adjusted assessment, if any, to the affected companies. <u>Any such domestic insurance company or other domestic entity may pay to the Insurance Commissioner the entire assessment required under this subsection in one payment when the first installment of such assessment is due.</u>

Sec. 5. Section 38a-591g of the general statutes is repealed and the following is substituted in lieu thereof (*Effective October 1, 2021*):

(a) (1) A covered person or a covered person's authorized representative may file a request for an external review or an expedited external review of an adverse determination or a final adverse

determination in accordance with the provisions of this section. All requests for external review or expedited external review shall be made in writing to the commissioner. The commissioner may prescribe the form and content of such requests.

[(2) (A) All requests for external review or expedited external review shall be accompanied by a filing fee of twenty-five dollars, except that no covered person or covered person's authorized representative shall pay more than seventy-five dollars in a calendar year for such covered person. Any filing fee paid by a covered person's authorized representative shall be deemed to have been paid by the covered person. If the commissioner finds that the covered person is indigent or unable to pay the filing fee, the commissioner shall waive such fee. Any such fees shall be deposited in the Insurance Fund established under section 38a-52a.

(B) The commissioner shall refund any paid filing fee to the covered person or the covered person's authorized representative, as applicable, or the health care professional if the adverse determination or the final adverse determination that is the subject of the external review request or expedited external review request is reversed or revised.**]**

[(3)**]** (2) The health carrier that issued the adverse determination or the final adverse determination that is the subject of the external review request or the expedited external review request shall pay the independent review organization for the cost of conducting the review.

[(4)**]** (3) An external review decision, whether such review is a standard external review or an expedited external review, shall be binding on the health carrier or a self-insured governmental plan and the covered person, except to the extent such health carrier or covered person has other remedies available under federal or state law. A covered person or a covered person's authorized representative shall not file a subsequent request for an external review or an expedited external review that involves the same adverse determination or final adverse determination for which the covered person or the covered person's authorized representative already received an external review

decision or an expedited external review decision.

[(5)**]** (4) Each health carrier shall maintain written records of external reviews as set forth in section 38a-591h.

[(6)**]** (5) Each independent review organization shall maintain written records as set forth in subsection (e) of section 38a-591m.

(b) (1) Except as otherwise provided under subdivision (2) of this subsection or subsection (d) of this section, a covered person or a covered person's authorized representative shall not file a request for an external review or an expedited external review until the covered person or the covered person's authorized representative has exhausted the health carrier's internal grievance process.

(2) A health carrier may waive its internal grievance process and the requirement for a covered person to exhaust such process prior to filing a request for an external review or an expedited external review.

(c) (1) At the same time a health carrier sends to a covered person or a covered person's authorized representative a written notice of an adverse determination or a final adverse determination issued by the health carrier, the health carrier shall include a written disclosure to the covered person and, if applicable, the covered person's authorized representative of the covered person's right to request an external review.

(2) The written notice shall include:

(A) The following statement or a statement in substantially similar language: "We have denied your request for benefit approval for a health care service or course of treatment. You may have the right to have our decision reviewed by health care professionals who have no association with us by submitting a request for external review to the office of the Insurance Commissioner, if our decision involved making a judgment as to the medical necessity, appropriateness, health care setting, level of care or effectiveness of the health care service or treatment you requested.";

(B) For a notice related to an adverse determination, a statement informing the covered person that:

(i) If the covered person has a medical condition for which the time period for completion of an expedited internal review of a grievance involving an adverse determination would seriously jeopardize the life or health of the covered person or would jeopardize the covered person's ability to regain maximum function, the covered person or the covered person's authorized representative may (I) file a request for an expedited external review, or (II) file a request for an expedited external review if the adverse determination involves a denial of coverage based on a determination that the recommended or requested health care service or treatment is experimental or investigational and the covered person's treating health care professional certifies in writing that such recommended or requested health care service or treatment would be significantly less effective if not promptly initiated; and

(ii) Such request for expedited external review may be filed at the same time the covered person or the covered person's authorized representative files a request for an expedited internal review of a grievance involving an adverse determination, except that the independent review organization assigned to conduct the expedited external review shall determine whether the covered person shall be required to complete the expedited internal review of the grievance prior to conducting the expedited external review;

(C) For a notice related to a final adverse determination, a statement informing the covered person that:

(i) If the covered person has a medical condition for which the time period for completion of an external review would seriously jeopardize the life or health of the covered person or would jeopardize the covered person's ability to regain maximum function, the covered person or the covered person's authorized representative may file a request for an expedited external review; or

(ii) If the final adverse determination concerns (I) an admission,

availability of care, continued stay or health care service for which the covered person received emergency services but has not been discharged from a facility, the covered person or the covered person's authorized representative may file a request for an expedited external review, or (II) a denial of coverage based on a determination that the recommended or requested health care service or treatment is experimental or investigational and the covered person's treating health care professional certifies in writing that such recommended or requested health care service or treatment would be significantly less effective if not promptly initiated, the covered person or the covered person's authorized representative may file a request for an expedited external review;

(D) (i) A copy of the description of both the standard and expedited external review procedures the health carrier is required to provide, highlighting the provisions in the external review procedures that give the covered person or the covered person's authorized representative the opportunity to submit additional information and including any forms used to process an external review or an expedited external review;

(ii) As part of any forms provided under subparagraph (D)(i) of this subdivision, an authorization form or other document approved by the commissioner that complies with the requirements of 45 CFR 164.508, as amended from time to time, by which the covered person shall authorize the health carrier and the covered person's treating health care professional to release, transfer or otherwise divulge, in accordance with sections 38a-975 to 38a-999a, inclusive, the covered person's protected health information including medical records for purposes of conducting an external review or an expedited external review;

(E) A statement that the covered person or the covered person's authorized representative may request, free of charge, copies of all documents, communications, information and evidence regarding the adverse determination or the final adverse determination that were not previously provided to the covered person or the covered person's

authorized representative.

(3) Upon request pursuant to subparagraph (E) of subdivision (2) of this subsection, the health carrier shall provide such copies in accordance with subsection (b) of section 38a-591n.

(d) (1) A covered person or a covered person's authorized representative may file a request for an expedited external review of an adverse determination or a final adverse determination with the commissioner, except that an expedited external review shall not be provided for a retrospective review request of an adverse determination or a final adverse determination.

(2) Such request may be filed at the time the covered person receives:

(A) An adverse determination, if:

(i) (I) The covered person has a medical condition for which the time period for completion of an expedited internal review of the adverse determination would seriously jeopardize the life or health of the covered person or would jeopardize the covered person's ability to regain maximum function; or

(II) The denial of coverage is based on a determination that the recommended or requested health care service or treatment is experimental or investigational and the covered person's treating health care professional certifies in writing that such recommended or requested health care service or treatment would be significantly less effective if not promptly initiated; and

(ii) The covered person or the covered person's authorized representative has filed a request for an expedited internal review of the adverse determination; or

(B) A final adverse determination if:

(i) The covered person has a medical condition where the time period for completion of a standard external review would seriously jeopardize

the life or health of the covered person or would jeopardize the covered person's ability to regain maximum function;

(ii) The final adverse determination concerns an admission, availability of care, continued stay or health care service for which the covered person received emergency services but has not been discharged from a facility; or

(iii) The denial of coverage is based on a determination that the recommended or requested health care service or treatment is experimental or investigational and the covered person's treating health care professional certifies in writing that such recommended or requested health care service or treatment would be significantly less effective if not promptly initiated.

(3) Such covered person or covered person's authorized representative shall not be required to file a request for an external review prior to, or at the same time as, the filing of a request for an expedited external review and shall not be precluded from filing a request for an external review, within the time periods set forth in subsection (e) of this section, if the request for an expedited external review is determined to be ineligible for such review.

(e) (1) Not later than one hundred twenty calendar days after a covered person or a covered person's authorized representative receives a notice of an adverse determination or a final adverse determination, the covered person or the covered person's authorized representative may file a request for an external review or an expedited external review with the commissioner in accordance with this section.

(2) (A) Not later than one business day after the commissioner receives a request that is complete, the commissioner shall: **[**send**]**

(i) Send a copy of such request to the health carrier that issued the adverse determination or the final adverse determination that is the subject of the request; **[**.**]** and

(ii) Assign an independent review organization from the list of

approved independent review organizations compiled and maintained by the commissioner pursuant to section 38a-591*l* to conduct the review and notify the health carrier of the name of the assigned independent review organization. Such assignment shall be done on a random basis among those approved independent review organizations qualified to conduct the particular review based on the nature of the health care service that is the subject of the adverse determination or the final adverse determination and other circumstances, including conflict of interest concerns as set forth in section 38a-591m.

(3) Not later than five business days after the health carrier receives the copy of an external review request or one calendar day after the health carrier receives the copy of an expedited external review request, from the commissioner, the health carrier shall complete a preliminary review of the request to determine whether:

(A) The individual is or was a covered person under the health benefit plan at the time the health care service was requested or, in the case of an external review of a retrospective review request, was a covered person in the health benefit plan at the time the health care service was provided;

(B) The health care service that is the subject of the adverse determination or the final adverse determination is a covered service under the covered person's health benefit plan but for the health carrier's determination that the health care service is not covered because **[**it**]** the health care service does not meet the health carrier's requirements for medical necessity, appropriateness, health care setting, level of care or effectiveness;

(C) If the health care service or treatment is experimental or investigational:

(i) Is a covered benefit under the covered person's health benefit plan but for the health carrier's determination that the service or treatment is experimental or investigational for a particular medical condition;

(ii) Is not explicitly listed as an excluded benefit under the covered person's health benefit plan;

(iii) The covered person's treating health care professional has certified that one of the following situations is applicable:

(I) Standard health care services or treatments have not been effective in improving the medical condition of the covered person;

(II) Standard health care services or treatments are not medically appropriate for the covered person; or

(III) There is no available standard health care service or treatment covered by the health carrier that is more beneficial than the recommended or requested health care service or treatment; and

(iv) The covered person's treating health care professional:

(I) Has recommended a health care service or treatment that the health care professional certifies, in writing, is likely to be more beneficial to the covered person, in the health care professional's opinion, than any available standard health care services or treatments; or

(II) Is a licensed, board certified or board eligible health care professional qualified to practice in the area of medicine appropriate to treat the covered person's condition and has certified in writing that scientifically valid studies using accepted protocols demonstrate that the health care service or treatment requested by the covered person that is the subject of the adverse determination or the final adverse determination is likely to be more beneficial to the covered person than any available standard health care services or treatments;

(D) The covered person has exhausted the health carrier's internal grievance process or the covered person or the covered person's authorized representative has filed a request for an expedited external review as provided under subsection (d) of this section; and

(E) The covered person has provided all the information and forms required to process an external review or an expedited external review, including an authorization form as set forth in subparagraph (D)(ii) of subdivision (2) of subsection (c) of this section.

(4) (A) Not later than one business day after the preliminary review of an external review request or the day the preliminary review of an expedited external review request is completed, the health carrier shall notify the commissioner, the covered person and, if applicable, the covered person's authorized representative in writing whether the request for an external review or an expedited external review is complete and eligible for such review. The commissioner may specify the form for the health carrier's notice of initial determination under this subdivision and any supporting information required to be included in the notice.

(B) If the external review or the expedited external review is accepted, the health carrier shall notify the commissioner, the covered person and, if applicable, the covered person's authorized representative in writing of the request's eligibility and acceptance for external review or expedited external review. For an external review, the health carrier shall include in such notice (i) a statement that the covered person or the covered person's authorized representative may submit, not later than five business days after the covered person or the covered person's authorized representative, as applicable, received such notice, additional information in writing to the assigned independent review organization that such organization shall consider when conducting the external review, and (ii) where and how such additional information is to be submitted. If additional information is submitted later than five business days after the covered person or the covered person's authorized representative, as applicable, received such notice, the independent review organization may, but shall not be required to, accept and consider such additional information.

[(B)**]** (C) If the request:

(i) Is not complete, the health carrier shall notify the commissioner

and the covered person and, if applicable, the covered person's authorized representative in writing and include in the notice what information or materials are needed to perfect the request; or

(ii) Is not eligible for external review or expedited external review, the health carrier shall notify the commissioner, the covered person and, if applicable, the covered person's authorized representative in writing and include in the notice the reasons for its ineligibility.

[(C)**]** (D) The notice of initial determination shall include a statement informing the covered person and, if applicable, the covered person's authorized representative that a health carrier's initial determination that the request for an external review or an expedited external review is ineligible for review may be appealed to the commissioner.

[(D)**]** (E) Notwithstanding a health carrier's initial determination that a request for an external review or an expedited external review is ineligible for review, the commissioner may determine, pursuant to the terms of the covered person's health benefit plan, that such request is eligible for such review and assign an independent review organization to conduct such review. Any such review shall be conducted in accordance with this section.

[(f) (1) Whenever the commissioner is notified pursuant to subparagraph (A) of subdivision (4) of subsection (e) of this section that a request is eligible for external review or expedited external review, the commissioner shall, not later than one business day after receiving such notice for an external review or one calendar day after receiving such notice for an expedited external review:

(A) Assign an independent review organization from the list of approved independent review organizations compiled and maintained by the commissioner pursuant to section 38a-591*l* to conduct the review and notify the health carrier of the name of the assigned independent review organization. Such assignment shall be done on a random basis among those approved independent review organizations qualified to conduct the particular review based on the nature of the health care

service that is the subject of the adverse determination or the final adverse determination and other circumstances, including conflict of interest concerns as set forth in section 38a-591m; and

(B) Notify the covered person and, if applicable, the covered person's authorized representative in writing of the request's eligibility and acceptance for external review or expedited external review. For an external review, the commissioner shall include in such notice (i) a statement that the covered person or the covered person's authorized representative may submit, not later than five business days after the covered person or the covered person's authorized representative, as applicable, received such notice, additional information in writing to the assigned independent review organization that such organization shall consider when conducting the external review, and (ii) where and how such additional information is to be submitted. If additional information is submitted later than five business days after the covered person or the covered person's authorized representative, as applicable, received such notice, the independent review organization may, but shall not be required to, accept and consider such additional information.**]**

[(2)**]** (f) (1) Not later than five business days for an external review or one calendar day for an expedited external review, after the health carrier **[**receives notice of the name of the assigned independent review organization from the commissioner**]** accepts the external review or expedited external review, the health carrier or its designee utilization review company shall provide to the assigned independent review organization the documents and any information such health carrier or utilization review company considered in making the adverse determination or the final adverse determination.

[(3)**]** (2) The failure of the health carrier or its designee utilization review company to provide the documents and information within the time specified in subdivision **[**(2)**]** (1) of this subsection shall not delay the conducting of the review.

[(4)**]** (3) (A) If the health carrier or its designee utilization review company fails to provide the documents and information within the

time period specified in subdivision [(2)] (1) of this subsection, the independent review organization may terminate the review and make a decision to reverse the adverse determination or the final adverse determination.

(B) Not later than one business day after terminating the review and making the decision to reverse the adverse determination or the final adverse determination, the independent review organization shall notify the commissioner, the health carrier, the covered person and, if applicable, the covered person's authorized representative in writing of such decision.

(g) (1) The assigned independent review organization shall review all the information and documents received pursuant to subsection (f) of this section. In reaching a decision, the independent review organization shall not be bound by any decisions or conclusions reached during the health carrier's utilization review process.

(2) Not later than one business day after receiving any information submitted by the covered person or the covered person's authorized representative pursuant to subparagraph (B) of subdivision [(1)] (4) of subsection [(f)] (e) of this section, the independent review organization shall forward such information to the health carrier.

(3) (A) Upon the receipt of any information forwarded pursuant to subdivision (2) of this subsection, the health carrier may reconsider its adverse determination or the final adverse determination that is the subject of the review. Such reconsideration shall not delay or terminate the review.

(B) The independent review organization shall terminate the review if the health carrier decides, upon completion of its reconsideration and notice to such organization as provided in subparagraph (C) of this subdivision, to reverse its adverse determination or its final adverse determination and provide coverage or payment for the health care service or treatment that is the subject of the adverse determination or the final adverse determination.

(C) Not later than one business day after making the decision to reverse its adverse determination or its final adverse determination, the health carrier shall notify the commissioner, the assigned independent review organization, the covered person and, if applicable, the covered person's authorized representative in writing of such decision.

(h) In addition to the documents and information received pursuant to subsection (f) of this section, the independent review organization shall consider, to the extent the documents or information are available and the independent review organization considers them appropriate, the following in reaching a decision:

(1) The covered person's medical records;

(2) The attending health care professional's recommendation;

(3) Consulting reports from appropriate health care professionals and other documents submitted by the health carrier, the covered person, the covered person's authorized representative or the covered person's treating health care professional;

(4) The terms of coverage under the covered person's health benefit plan to ensure that the independent review organization's decision is not contrary to the terms of coverage under such health benefit plan;

(5) The most appropriate practice guidelines, which shall include applicable evidence-based standards and may include any other practice guidelines developed by the federal government, national or professional medical societies, medical boards or medical associations;

(6) Any applicable clinical review criteria developed and used by the health carrier or its designee utilization review company; and

(7) The opinion or opinions of the independent review organization's clinical peer or peers who conducted the review after considering subdivisions (1) to (6), inclusive, of this subsection.

(i) (1) The independent review organization shall notify the

commissioner, the health carrier, the covered person and, if applicable, the covered person's authorized representative in writing of its decision to uphold, reverse or revise the adverse determination or the final adverse determination, not later than:

(A) For external reviews, forty-five calendar days after such organization receives the assignment from the commissioner to conduct such review;

(B) For external reviews involving a determination that the recommended or requested health care service or treatment is experimental or investigational, twenty calendar days after such organization receives the assignment from the commissioner to conduct such review;

(C) For expedited external reviews, except as specified under subparagraph (D) of this subdivision, as expeditiously as the covered person's medical condition requires, but not later than forty-eight hours after such organization receives the assignment from the commissioner to conduct such review or seventy-two hours after such organization receives such assignment if any portion of such forty-eight-hour period falls on a weekend;

(D) For expedited external reviews involving a health care service or course of treatment specified under subparagraph (B) or (C) of subdivision (38) of section 38a-591a, as expeditiously as the covered person's medical condition requires, but not later than twenty-four hours after such organization receives the assignment from the commissioner to conduct such review; and

(E) For expedited external reviews involving a determination that the recommended or requested health care service or treatment is experimental or investigational, as expeditiously as the covered person's medical condition requires, but not later than five calendar days after such organization receives the assignment from the commissioner to conduct such review.

(2) Such notice shall include:

(A) A general description of the reason for the request for the review;

(B) The date the independent review organization received the assignment from the commissioner to conduct the review;

(C) The date the review was conducted;

(D) The date the organization made its decision;

(E) The principal reason or reasons for its decision, including what applicable evidence-based standards, if any, were used as a basis for its decision;

(F) The rationale for the organization's decision;

(G) Reference to the evidence or documentation, including any evidence-based standards, considered by the organization in reaching its decision; and

(H) For a review involving a determination that the recommended or requested health care service or treatment is experimental or investigational:

(i) A description of the covered person's medical condition;

(ii) A description of the indicators relevant to determining whether there is sufficient evidence to demonstrate that (I) the recommended or requested health care service or treatment is likely to be more beneficial to the covered person than any available standard health care services or treatments, and (II) the adverse risks of the recommended or requested health care service or treatment would not be substantially increased over those of available standard health care services or treatments;

(iii) A description and analysis of any medical or scientific evidence considered in reaching the opinion;

(iv) A description and analysis of any evidence-based standard; and

(v) Information on whether the clinical peer's rationale for the opinion is based on the documents and information set forth in subsection (f) of this section.

(3) Upon the receipt of a notice of the independent review organization's decision to reverse or revise an adverse determination or a final adverse determination, the health carrier shall immediately approve the coverage that was the subject of the adverse determination or the final adverse determination.

This act shall take effect as follows and shall amend the following sections:		
Section 1	*July 1, 2021*	19a-7p(b) and (c)
Sec. 2	*from passage*	38a-12
Sec. 3	*from passage*	38a-38(b) to (g)
Sec. 4	*July 1, 2021*	38a-48(g)
Sec. 5	*October 1, 2021*	38a-591g

INS *Joint Favorable Subst.*

The following Fiscal Impact Statement and Bill Analysis are prepared for the benefit of the members of the General Assembly, solely for purposes of information, summarization and explanation and do not represent the intent of the General Assembly or either chamber thereof for any purpose. In general, fiscal impacts are based upon a variety of informational sources, including the analyst's professional knowledge. Whenever applicable, agency data is consulted as part of the analysis, however final products do not necessarily reflect an assessment from any specific department.

OFA Fiscal Note

State Impact:

Agency Affected	Fund-Effect	FY 22 $	FY 23 $
Insurance Dept.	GF - Potential Revenue Gain	Minimal	Minimal
Insurance Dept.	IF - Net Savings	2,550	3,400

Note: GF=General Fund; IF=Insurance Fund

Municipal Impact: None

Explanation

The bill makes a variety of changes to the insurance statutes that result in the fiscal impacts below.

The bill results in a potential minimal revenue gain to the General Fund from additional penalties and fines related to the Public Health Fee. Under the bill, the Insurance Commissioner may assess a civil fine of up to $15,000 on insurers and HMO's that intentionally misrepresent the number of covered lives under their policies. The bill also establishes a late filing fee of $100 per day. As the Insurance Department (DOI) does not have issues with the accurate and timely submission by insurers and HMO's for the Public Health Fee, there is minimal, if any, new revenue anticipated from these provisions.

The bill results in a net savings for DOI of approximately $3,400 per year due to the elimination of the $25 external review application fee because the agency currently spends more on fee administration than it gains in revenue. For example, DOI collected $5,759 in such fees in 2020 but had to return fees worth $3,800 because the fee is waived in certain cases. The resulting fee revenue in 2020 of $1,959 was more than offset

by the $5,340 incurred by DOI in administrative costs for the handling of initial and returned checks.[1] The FY 22 fiscal impact reflects nine months of net savings.

The bill allows domestic insurance companies to pay their entire share of the Insurance Fund General Assessment at the first payment date rather than quarterly, which may bring forward some Insurance Fund revenue but does not change the total revenue amount to be received by the fund.

The bill also makes technical changes to the insurance data security law and repeals a reporting requirement for the Insurance Commissioner, both of which have no fiscal impact. For the annual report being repealed, neither the information it is intended to report about nor the report itself has been submitted in recent years.

The Out Years

The annualized ongoing fiscal impact identified above would continue into the future subject to the amount of applications for external review and any penalties related to the Public Health Fee assessed.

Sources: Connecticut Insurance Department

[1] According to DOI, they incur a cost of $10 per check for initial fees and $20 per check for refunds.

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)