STATE OF CONNECTICUT

INSURANCE DEPARTMENT

Bulletin IC - 42
July 20, 2020

TO: All Licensees of the Connecticut Insurance Department

RE: Connecticut Insurance Data Security Law

On June 4, 2019, the Connecticut General Assembly enacted the Insurance Data Security Law ("Act"), now codified as Conn. Gen. Stat. § 38a-38, which becomes effective October 1, 2020.[1] The Act establishes standards applicable to licensees of the Connecticut Insurance Department for data security, the investigation of a cybersecurity event, and notification to the Department of such event.[2] This bulletin is intended to provide licensees with guidance for compliance with its provisions.

Scope: The Act applies to all persons who are licensed, authorized to operate or registered, or required to be licensed, authorized or registered pursuant to the insurance laws of Connecticut, except for purchasing groups or risk retention groups chartered and licensed in another state or a licensee that is acting as an assuming insurer and domiciled in another state or jurisdiction.[3]

Information Security Program: Licensees must develop, implement and maintain a comprehensive written information security program ("ISP") that complies with the requirements of Conn. Gen. Stat. § 38a-38(c) not later than **October 1, 2020**. The ISP must be based on the licensee's risk assessment and contain safeguards for the protection of nonpublic information and the licensee's information systems[4] commensurate with the size and complexity of the licensee, its activities, including use of

---

[1] See **Public Act No. 19-117, Sections 230-231 & 431 (approved June 26, 2019), as amended by Public Act No. 19-196, Sections 8 & 9 (approved July 8, 2019).**

[2] Connecticut had previously enacted legislation in 2015, codified as Conn. Gen. Stat. § 38a-999b, applicable to health insurers, health care centers, pharmacy benefits managers, third-party administrators administering health benefits, and utilization review companies, which requires such entities to implement and maintain by October 1, 2017, a comprehensive information security program to safeguard the personal information the entity compiles or maintains on insureds and enrollees, and specifies security program requirements, notice requirements for actual or suspected breach of security, and annual certification to the insurance Commissioner of the entity's compliance with this statute. Conn. Gen. Stat. § 38a-999b, is repealed effective October 1, 2021.

[3] The Insurance Department interprets the definition of "licensee" in Conn. Gen. Stat. § 38a-38(b)(7) as not including a Commissioner of the Superior Court acting as a title agent as defined in Conn. Gen. Stat. § 38a-402.

[4] The Department interprets the definition of "information system" in Conn. Gen. Stat. § 38a-38(b)(6) as meaning 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 systems, telephone switching and private branch exchange system, and environmental control system.

third-party service providers, and the sensitivity of the nonpublic information[5] used by the licensee or in its possession, custody or control. Some licensees are excepted from compliance with these requirements pursuant to Conn. Gen. Stat. § 38a-38(c)(10).

Third-Party Service Providers: Unless the licensee falls within an exception specified in Conn. Gen. Stat. § 38a-38(c)(10), licensees must exercise due diligence in selecting third-party service providers ("TPSPs"), and not later than **October 1, 2021**, must require each of the licensee's TPSPs to implement appropriate administrative, technical, and physical measures to protect and secure the information systems and nonpublic information that is accessible to, or held by, the licensee's TPSPs.

Annual Certification by Domestic Insurers: Beginning **February 15, 2021**, annually, Connecticut domestic insurers and health care centers[6] must submit a written statement to the Insurance Commissioner certifying that the insurer is in compliance with the requirements of Conn. Gen. Stat. § 38a-38(c), unless the insurer or health care center falls within an exception specified in Conn. Gen. Stat. § 38a-38(c)(10). All records, schedules and data supporting each such certification must be maintained for examination by the Insurance Department for a period of five years. A domestic insurer or health care center that is a member of an insurance holding company system may submit one statement certifying compliance with the requirements of Conn. Gen. Stat. § 38a-38(c) to the Insurance Commissioner on behalf of other domestic insurers or health care centers that are members of the same holding company system. To the extent the insurer or health care center has identified areas, systems or processes that require material improvement, updating or redesign, the insurer or health care center shall, either directly or through an affiliate, document such identification and remedial efforts planned and underway to address such areas, systems or processes and make such documentation available for inspection by the Insurance Department.

Exceptions: The Act specifies the following exceptions to the requirements of Conn. Gen. Stat. § 38a-38(c):

> **Small licensees:** Beginning **October 1, 2020** and ending **September 30, 2021**, each licensee with fewer than twenty (20) employees (including independent contractors having access to the nonpublic information used by the licensee or in the possession, custody or control of the licensee). On or after **October 1, 2021**, each licensee with fewer than ten (10) employees (including independent contractors having access to the nonpublic information used by the licensee or in the possession, custody or control of the licensee).[7]
>
> **HIPPA compliant licensees:** Each licensee that has established and maintains an ISP that is compliant with the Health Insurance Portability and Accountability Act of 1996 and the rules, regulations, procedures or guidelines established

[5] The Department interprets the definition of "nonpublic information" in Conn. Gen. Stat. § 38a-38(b)(9) as relating to electronic data and information.

[6] The reference to domestic insurers in Conn. Gen. Stat. § 38a-38(c)(9) is interpreted by the Insurance Department to include domestic health care centers.

[7] Conn. Gen. Stat. § 38a-38(c)(10)(A)(i).

thereunder, and submits to the Insurance Commissioner a written statement certifying such licensee's compliance therewith.[8]

Licensee employees and agents: Each employee, agent, representative or designee of a licensee, who is also a licensee.[9]

Licensees from approved jurisdictions: 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 Insurance Commissioner pursuant to regulations adopted pursuant to the Act, provided such licensee submits to the Commissioner, not later than **February 15th**, annually, a written statement certifying such licensee's compliance therewith.[10]

In the event that a licensee ceases to qualify for an exception to the requirements of Conn. Gen. Stat. § 38a-38(c), the licensee will have 180 days to comply with this subsection.[11]

Cybersecurity Event Investigations: When a licensee learns that a cybersecurity event[12] has or may have occurred, the licensee or an outside vendor or service provider designated to act on behalf of such licensee, must conduct a prompt investigation in accordance with the provisions of Conn. Gen. Stat. § 38a-38(d). These provisions include: determining whether a cybersecurity event occurred; if a cybersecurity event has occurred, assess the nature and scope of the cybersecurity event; identify if any nonpublic information[13] may have been involved in such cybersecurity event; and perform measurers to restore the security of the information in order to prevent further unauthorized acquisition, release or use of nonpublic information that is in the licensee's possession, custody or control.

If a licensee learns that a cybersecurity event has or may have occurred in a system maintained by a TPSP, the licensee must conduct an investigation completing the steps described in Conn. Gen. Stat. § 38a-38(d)(2) or confirm and document that the TPSP has completed the such steps.

---

[8] Conn. Gen. Stat. § 38a-38(c)(10)(A)(ii).

[9] Conn. Gen. Stat. § 38a-38(c)(10)(A)(iii).

[10] Conn. Gen. Stat. § 38a-38(c)(10)(A)(iv).

[11] Conn. Gen. Stat. § 38a-38(c)(10)(B).

[12] The Insurance Department interprets the definition of "cybersecurity event" in Conn. Gen. Stat. § 38a-38(b)(3) as meaning 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.

[13] See footnote 5 of this bulletin.

Each licensee shall maintain records concerning each cybersecurity event for at least five (5) years from the date of the event, and shall produce such records to the Insurance Commissioner upon demand by the Commissioner.

Notification of a Cybersecurity Event:

Notification to the Commissioner:[14] Each licensee shall notify the Insurance Commissioner that a cybersecurity event has occurred, as promptly as possible but in no event later than three (3) business days after the date of the cybersecurity event,[15] when either:

1) Connecticut is, in the case of an insurer, the state of domicile, or, in the case of a producer, the licensee's home state;[16]

2) The licensee reasonably believes that the cybersecurity event involves nonpublic information of 250 or more consumers residing in this state and the event: (a) state or federal laws requires that a notice concerning the cybersecurity event be provided to a government body, self-regulatory agency or another supervisory body; or (b) has a reasonable likelihood of materially harming any consumer residing in Connecticut or a material part of the licensee's normal operations.

Notification to the Commissioner of a cybersecurity event shall be reported to the Commissioner in an electronic form which shall be available on the Insurance Department's website by October 1, 2020.[17]

If a licensee is affected by a cybersecurity event in an information system maintained by a TPSP, the licensee is required to treat such event as requiring notice to the Commissioner, if the licensee has actual knowledge of the event. However, the licensee may allow the TPSP to provide the required notice to the Commissioner.[18]

Notification to Consumers:[19] The Act requires each licensee to comply with all applicable provisions of Conn. Gen. Stat. § 36a-701b (Connecticut's data breach notification law), which requires any person who conducts business in this state

[14] Conn. Gen. Stat. § 38a-38(e)(1).

[15] The Insurance Department interprets "after the date of the cybersecurity event" as meaning after the date on which the licensee first determines that a cybersecurity event has occurred.

[16] Notice to the Insurance Department by such licensees should relate to a cybersecurity event that has a reasonable likelihood of materially harming a consumer residing in this state or a reasonable likelihood of materially harming any material part of the normal operations of the licensee.

[17] Conn. Gen. Stat. § 38a-38(e)(2).

[18] Conn. Gen. Stat. § 38a-38(3)(4). The three (3) business day deadline to report the event to the Insurance Commissioner begins on the day after a TPSP notifies the licensee of the cybersecurity event or such licensee becomes aware of such event, whichever is sooner.

[19] Conn. Gen. Stat. § 38a-38(e)(3).

and who in the ordinary course of business owns, licenses or maintains computerized data that contains personal information of any resident of this state, to disclose any breach of security to all affected individuals as set forth therein. The licensee shall also provide the Insurance Commissioner a copy of the notice the licensee sends to consumers if the licensee is required to notify the Commissioner as described above.

Notice Regarding Cybersecurity Events of Reinsurers:[20] The Act requires licensees acting as an assuming insurer to notify affected ceding insurers and its domiciliary regulator of a cybersecurity event involving nonpublic information that is used by such assuming insurer or in its possession, custody or control when it is acting as an assuming insurer with no direct contractual relationship with affected consumers not later than **72 hours** after the assuming insurer discovered that the cybersecurity event has occurred. 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 Conn. Gen. Stat. § 36a-701b (Connecticut's data breach notification law) and comply with any other applicable notification requirements imposed under the Act.

The Act also requires licensees acting as an assuming insurer to notify affected ceding insurers and its domiciliary regulator of a cybersecurity event involving nonpublic information that in the possession, custody or control of a TPSP of the licensee not later than **72 hours** after the assuming insurer received notice from the TPSP disclosing that the cybersecurity event occurred. Ceding insurers that have a direct contractual relationship with affected consumers shall fulfill the consumer notification requirements imposed under Conn. Gen. Stat. § 36a-701b (Connecticut's data breach notification law) and comply with any other applicable notification requirements imposed under the Act.

Notice by Insurers to Producers of Record:[21] If the cybersecurity event involves nonpublic information that is in the possession, custody or control of an licensee acting as insurer or a TPSP for an insurer, the Act requires the insurer to notify the producer of record for any affected consumer residing in this state who accessed services through an independent insurance producer of the occurrence of such event not later than the time at which notice is provided to such consumer, provided the insurer has the current producer of record information for such individual consumer.

Licensee Compliance: The Act grants the Insurance Commissioner the power to examine and investigate licensees to determine compliance with the Act, and to impose penalties for noncompliance.[22] In recognition of the impact of COVID-19 on licensees of

[20] Conn. Gen. Stat. § 38a-38(e)(5).

[21] Conn. Gen. Stat. § 38a-38(e)(6).

[22] Conn. Gen. Stat. § 38a-38(f). The power of the Commissioner under this subsection is in addition to the Commissioner's powers under Conn. Gen. Stat. §§ 38a-14 to 38a-16, inclusive.

the Insurance Department and their employees, the Department intends to exercise appropriate discretion in evaluating the facts and circumstances of a licensee's compliance with the provisions of the Act and in the imposition of sanctions for non-compliance.

In this regard, the Department will not impose sanctions upon a licensee that fails to file with the Insurance Commissioner its annual certification of compliance required by Conn. Gen. Stat. § 38a-38(c)(9) or § 38a-38(c)(10) by the February 15, 2021 due date provided the certification of compliance is filed by April 15, 2021.

Any licensee that is unable to timely comply with the requirements of the Act due to circumstances related to the current COVID-19 situation is urged to contact the Insurance Department Market Conduct Division at cid.mc@ct.gov and provide a description of the reasons why, despite reasonable efforts expended to comply with the requirements of the Act, the licensee is unable to satisfy the requirements of the Act.

Bulletin IC-25: Insurance Department Bulletin IC-25 dated August 18, 2010 is hereby rescinded effective October 1, 2020. This is to coincide with the effective date of the Act.

Bulletin MC-23: Insurance Department Bulletin MC-23 dated June 13, 2017 is hereby rescinded effective October 1, 2021. This is to coincide with the repeal of Conn. Gen. Stat. § 38a-999b effective October 1, 2021.

Please contact the Insurance Department Market Conduct Division at cid.mc@ct.gov with any questions.

Andrew N. Mais
Insurance Commissioner