STATE OF CONNECTICUT

INSURANCE DEPARTMENT

BULLETIN IC - 25
August 18, 2010

TO: All Regulated Entities in Connecticut, including, Insurance Producers, Public Adjusters, Bail Bond Agents, Appraisers, Certified Insurance Consultants, Casualty Claim Adjusters, Property and Casualty Insurers, Life and Health Insurers, Health Care Centers, Fraternal Benefit Societies, Captive Insurers, Utilization Review Companies, Risk Retention Groups, Surplus Line Companies, Life Settlement Companies, Preferred Provider Networks, Pharmacy Benefit Managers, and Medical Discount Plans

RE: Information Security Incidents

In order to assure that Connecticut consumers are fully protected and informed in the event of any information security incident, as defined below, that could pose a potential risk to the privacy of an individual's personal health and/or financial information, the Connecticut Insurance Department ("Department") is requiring that all licensees and registrants of the Department notify the Department of any information security incident which affects any Connecticut residents as soon as the incident is identified, but no later than five (5) calendar days after the incident is identified. Notification should be sent to the Insurance Commissioner ("Commissioner") in writing via first class mail, overnight delivery service or electronic mail.

The Department understands and even expects that with the overwhelming amount of information obtained and maintained by all businesses that there will be at times information security incidents which are beyond the control of the best management practices. The Department's concern is to make certain that in addition to minimizing these incidents, licensees and registrants react quickly and affirmatively to let affected Connecticut consumers know that they may be at risk and what is being done to protect sensitive and confidential information. The Department also wants to make sure that there is an opportunity for the Department to actively monitor the situation and guarantee those consumer protections throughout the process.

AUTHORITY TO COMPEL NOTIFICATION

The authority to compel this notification to the Department is provided to the Commissioner under Conn. Gen. Stat. §38a-8 which provides the Commissioner with "all powers specifically granted, and all further powers that are reasonable and necessary to enable the commissioner to protect the public interest" in accordance with the duties imposed on the Commissioner by the insurance statutes. To maintain licenses to do business in Connecticut, insurers and health care centers are required to exhibit evidence of good management as required by Conn. Gen. Stat. §38a-41. The other licensee and registrant entities have similar requirements to do business in Connecticut. [1] In addition,

[1] Relevant Conn. Gen. Stat. §§: 38a-465- Life Settlement Brokers and Life Settlement Companies; 38a-479aa – Preferred Provider Network; 38a-479rr – Medical Discount Plans; 38a-702b – Producers; 38a-660 – Bail Bond agents; 38a-769 - Public Adjuster, Casualty Adjuster, Motor Vehicle Physical Damage Appraiser, Certified Insurance Consultant, Surplus

Conn. Gen. Stat. §38a-478o requires that each managed care organization shall conform to all applicable state and federal antidiscrimination and confidentiality statutes, shall ensure that the confidentiality of specified enrollee patient information and records in its custody is protected, and shall have written confidentiality policies and procedures and sections 38a-8-124 through 38a-126, inclusive, of the Regulations of Connecticut State Agencies provides requirements for safeguarding customer financial information.

In addition to the authority of the Commissioner under the insurance laws, the Commissioner has been given additional authority to protect the personal information of insurance consumers pursuant to the relevant portions of Conn. Gen. Stat. §42-471:

(a) Any person in possession of personal information of another person shall safeguard the data, computer files and documents containing the information from misuse by third parties, and shall destroy, erase or make unreadable such data, computer files and documents prior to disposal.

(c) As used in this section, "personal information" means information capable of being associated with a particular individual through one or more identifiers, including, but not limited to, a Social Security number, a driver's license number, a state identification card number, an account number, a credit or debit card number, a passport number, an alien registration number or a health insurance identification number, and does not include publicly available information that is lawfully made available to the general public from federal, state or local government records or widely distributed media.

(d) For persons who hold a license, registration or certificate issued by a state agency other than the Department of Consumer Protection, this section shall be enforceable only by such other state agency pursuant to such other state agency's existing statutory and regulatory authority.

INFORMATION SECURITY INCIDENT DEFINED

The Department considers an information security incident to be any unauthorized acquisition or transfer of, or access to, personal health, financial, or personal information, whether or not encrypted, of a Connecticut insured, member, subscriber, policyholder or provider, in whatever form the information is collected, used or stored, which is obtained or maintained by a licensee or registrant of the Insurance Department, the loss of which could compromise or put at risk the personal, financial, or physical well being of the affected insureds, members, subscribers, policyholders or providers.

NOTIFICATION PROCEDURES

Any information security incident which affects any Connecticut resident must be reported in writing to the Commissioner as soon as the incident is identified, but not later than five

---

Lines Broker or any insurance-related occupation for which a license is deemed necessary by the commissioner, other than an occupation as an insurance producer; 38a-603 and 620 – fraternal societies may not operate in a manner which is hazardous to its members, creditors or public; Conn. Agencies Regs. § 38a-740-4(h) – standards for eligible surplus lines insurers.

(5) calendar days after the incident is identified. Notification should include as much the following as is known:

- Date of the incident
- Description of incident (how information was lost, stolen, breached)
- How discovered
- Has lost, stolen, or breached information been recovered and if so, how
- Have individuals involved in the incident (both internal and external) been identified
- Has a police report been filed
- Type of information lost, stolen, or breached (equipment, paper, electronic, claims, applications, underwriting forms, medical records etc)
- Was information encrypted
- Lost, stolen or breached information covers what period of time
- How many Connecticut residents affected
- Results of any internal review identifying either a lapse in internal procedures or confirmation that all procedures were followed
- Identification of remedial efforts being undertaken to cure the situation which permitted the information security incident to occur.
- Copies of the licensee/registrants Privacy Policies and Data Breach Policy.
- Regulated entity contact person for the Department to contact regarding the incident. (This should be someone who is both familiar with the details and able to authorize actions for the licensee or registrant)
- Other regulatory or law enforcement agencies notified (who, when)

The Department will want to review, in draft form, any communications proposed to be made to affected insureds, members, subscribers, policyholders or providers advising them of the incident. Depending on the type of incident and information involved, the Department will also want to have discussions regarding the level of credit monitoring and insurance protection which the Department will require to be offered to affected consumers and for what period of time.

The Department Market Conduct Division has the responsibility for monitoring the activities associated with any information security incident and will contact the designated licensee or registrant contact for additional information as necessary and to set up a monitoring process. Because each incident is unique, each monitoring process will be unique.

VENDORS / BUSINESS ASSOCIATES

The Department also considers that an information security incident at or by a vendor or business associate of a licensee or registrant, which has the potential of affecting personal health, financial, or personal information of a Connecticut insured, member, subscriber, policyholder or provider of a licensee or registrant should be reported by the licensee or registrant to the Department. The Department will want to be kept informed of how the licensee or registrant is managing the vendor's/business associate's activities

and what protections and remedies are being put in place by the vendor/business associate for the Connecticut consumers.

ADMINISTRATIVE ACTIONS

Each incident will be evaluated on its own merits and depending on the circumstances, some situations may warrant imposition of administrative penalties by the Department. To minimize that potential, licenses and registrants are urged to follow these procedures.

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

Thomas R. Sullivan
Insurance Commissioner