Last week, the Connecticut Insurance Commissioner issued Bulletin IC-25 which mandates that entities within its jurisdiction notify the Department of Insurance of any "information security incident." This email provides a brief summary of this new requirement.

Who must provide the notice?

The Bulletin applies to all licensees and registrants of the Department. This generally means all entities regulated by the Insurance Department, 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.

Additionally, in cases where the information security incident happens at a vendor or business associate, the Department expects to be notified of the incident as well as 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.

What is an "information security incident"?

Under this Bulletin, an information security incident is:

> 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.

Thus, unlike the general Connecticut data breach notification statute which requires notification only with respect to computerized personal information, this mandate applies to paper documents which includes personal health, financial or personal information. Also, encrypted data is **not** exempt from this notification requirement.

What is personal health, financial, or personal information?

The Bulletin does not define this term and, therefore, is unclear in this regard. However, in discussing its authority to impose the requirement, the Department cites to Conn. Gen. Stat. §42-471, which defines "personal information" to mean:
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.

This definition, however, may not be as broad as how the Department views the term "personal health, financial or personal information." Licensees and registrants should be careful here and err on the side of being more inclusive when deciding whether an incident needs to be handled in accordance with this Bulletin.

When must notification be provided?

The Bulletin requires licensees and registrants of the Department to notify it of the incident as soon as the incident is identified, **but no later than five (5) calendar days** after the incident is identified.

Where should notice be sent?

Notification should be sent to the Insurance Commissioner in writing via first class mail, overnight delivery service or electronic mail.

What must the notice include?

Notification should include as much information as is known concerning the incident. The Bulletin provides the following list of items of information to be reported to the Department:

- 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)

One of the items on this list to note is a Data Breach Policy which all entities should consider adopting even if not subject to this Bulletin.

Does the Department require that credit monitoring be offered in the event of an information security incident?

It looks like the Department may require credit monitoring in some circumstances. The Bulletin states that:

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. In addition, the Department wants to review the draft letters informing individuals of the information security incident.

Will the Department impose penalties?

The Bulletin states that the Department will evaluate each incident independently based on the applicable circumstances, and notes that some situations may warrant imposition of administrative penalties. The Department urges licenses and registrants to follow these procedures in order to minimize the possibility for penalties.

Licensees and registrants will need to review this guidance and incorporate it into their information security programs. Other entities should take note of this development and recognize the increasing efforts by federal and state agencies to safeguard personal information.