Privacy, Data Security
& Information Use

September 16, 2010

Data Breach Notification Burden Grows With First State Insurance Commissioner Mandate

by John L. Nicholson and Meighan E. O'Reardon

Effective August 18, 2010, any entity licensed by or registered with the Connecticut Department of Insurance must notify the Connecticut Insurance Commissioner within five days of an "information security incident" involving a Connecticut resident's personal health, financial or personal information that places such resident at risk.[1] Connecticut's insurance notification mandate is the first such measure by a state, adding to the already tangled web of state and Federal data breach notification standards and requirements.

On August 18, 2010, the Connecticut Insurance Commissioner issued Bulletin IC-25, officially requiring all entities subject to the jurisdiction of the Connecticut Department of Insurance to "notify the Department of any information security incident[s]" involving a Connecticut resident's personal health, financial or personal information "the loss of which could compromise or put at risk the personal, financial or physical well being of" the affected Connecticut residents.[2] The involvement of insurance regulators in the realm of data security incident definition and notification further complicates the maze of laws and regulations applying to security breaches, especially when entities regulated by the Insurance Commissioner are already subject to the Connecticut data breach notification law[3] and are likely covered by the data breach notification requirements included in the HITECH Act.[4]

Who Is Covered?

The requirements of Bulletin IC-25 (the "Insurance Requirements") apply to all licensees and registrants of the Connecticut Insurance Department. The entities required to comply encompass a variety of organizations including (but not limited to) property and casualty insurers, life and health insurers, health care

1 State of Connecticut Insurance Department, Bulletin IC-25 (August 18, 2010), available at http://www.ct.gov/cid/lib/cid/Bulletin_IC_25_Data_Breach_Notification.pdf.

2 *Id.* at 2.

3 CONN. GEN. STAT. § 36a-701(b).

4 Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009).

centers, captive insurers, life settlement companies, bail bond agents, appraisers, certified insurance consultants, casualty claim adjusters, fraternal benefit societies, pharmacy benefit managers, and medical discount plans ("Regulated Entities"). IC-25 also requires that Regulated Entities notify the Department if an information security incident that has the potential to affect the personal information of customers of the Regulated Entity who are Connecticut residents occurs at one of their vendors or business associates.[5] According to the Insurance Requirements, the Department wants 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 into place by the vendor/business associate for the Connecticut customers.[6]

When Do The Insurance Requirements Apply?

Definition of Personal Information

The Insurance Requirements use a broad definition of personal information. Unlike state data breach notification statutes and other information protection laws, IC-25 does not explicitly define personal information. The mandate states that notice is required if "personal health, financial or personal information" is put at risk by an information security incident. Given such a broad definition, looking to other aspects of CT law is helpful. IC-25 cites the Department's authority to protect personal information of insurance consumers under Conn. Gen. Stat. § 42-471 (Protection of Social Security Numbers and Personal Information).[7] Section 42-471(c) defines personal information as: "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."[8] Given the Department's reference to "personal health and financial information" in the mandate, Regulated Entities can reasonably assume that the type of information covered by this mandate is even broader than that listed in § 42-471.

Definition of Information Security Incident

The Insurance Requirements are triggered upon the occurrence of an "information security incident," which IC-25 defines as: "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, policy holder 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."[9] The phrase "could compromise or put at risk" is an interesting threshold. The standard appears to fall in the middle of the spectrum used in the various state data breach notification laws, with those like California's[10] that require notice to consumers of any unauthorized disclosure of or access to personal information at one end, and those like Maryland's[11] that only require notice to consumers if misuse of the personal information has occurred or is reasonably likely to occur. Significantly, the

[5] IC-25 uses the generic term "vendors/business associates." This appears to be broader than the HIPAA-definition of Business Associates.

[6] Bulletin IC-25 at 3-4.

[7] Conn. Gen. Stat. § 42-471 (2009).

[8] *Id.* at § 42-471(c).

[9] *Bulletin IC-25* at 2.

[10] Cal. Civ. Code § 1798.82

[11] Md. Code, Com. Law § 14-3504. Security breach.

mandate applies not just to breaches of information in electronic format but also to paper documents that include personal information.

Notification to the Commissioner is required regardless of whether the compromised information was encrypted. The use of the "at risk" provision without the exclusion for encrypted information could be an attempt to address the perceived flaws in many of the state data breach notification laws where, theoretically, weak encryption schemes could be used to obey the letter of the law and avoid the notice requirement without actually providing significant protection to consumer data. By using the "at risk" standard, the Insurance Requirements force Regulated Entities to stay abreast of developments in information security and use up-to-date encryption schemes that actually keep the data from being "at risk."

What Do Regulated Entities Have To Do?

Under the Insurance Requirements, if a Regulated Entity experiences an information security incident that affects any Connecticut resident, the incident must be reported to the Connecticut Insurance Commissioner as soon as the incident is identified, but no later than five (5) calendar days after discovery. Notice must be sent to the Connecticut Insurance Commissioner in writing via (i) first class mail, overnight delivery, or (ii) electronic mail. In the case of a security incident at a Regulated Entity's vendor or business associate, the Department requests additional information about how the Regulated Entity is managing the third party's response to the event.

The notification to the Commissioner should include the following:

1. date of the incident;
2. description of the incident;
3. how the incident was discovered;
4. whether the lost, stolen or breached information has been recovered, and if so, how;
5. whether individuals involved in the incident have been identified;
6. whether a police report was filed;
7. the type of information lost, stolen or breached;
8. whether the compromised information was encrypted;
9. the period of time covered by the compromised information;
10. how many Connecticut residents are affected;
11. the results of any internal review identifying either a lapse in internal procedures or confirmation that all procedures were followed;
12. identification of remedial efforts being undertaken to cure the situation which permitted the information security event to occur;

13. copies of the licensee/registrant's privacy policies and data breach policy;

14. the Regulated Entity's contact person for the Department to contact regarding the incident; and

15. the names of other regulatory or law enforcement agencies notified, including when such agencies were notified.

Bulletin IC-25 also includes some other notable compliance instructions. After notice is provided to the Insurance Commissioner, the Department intends to review any communications proposed to be made to affected insureds, members, subscribers, policy holders or providers advising them of the incident. The Department also clarified that it may 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."[12] Finally, and perhaps most significantly, the Bulletin states that some reported security incidents may result in administrative penalties, but offers little additional information regarding the triggers for such fines except to state, “To minimize that potential, licensees and registrants are urged to follow these procedures.”[13]

Relationship to Connecticut and HITECH Act Data Breach Notification Requirements

Bulletin IC-25 imposes requirements in addition to data breach notification requirements applicable under Connecticut’s data breach notification law and the HITECH Act.

Insurance Requirements vs. CT Data Breach Notification Law

In a few instances the Insurance Requirements are more stringent or even contradict the requirements of those other regimes. Among other things, the Connecticut data breach notification law only requires notice when computerized personal information is disclosed, while the Insurance Requirements apply to information “in whatever form the information is collected,” which could be electronic, paper or even verbal form. Furthermore, the Connecticut data breach notification statute only requires notice when personal information is compromised "that has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable."[14] The Insurance Requirements, on the other hand, apply regardless of whether the information was encrypted. The language in the Bulletin also indicates that the Insurance Commissioner may mandate that credit monitoring and other identity protection services be offered to customers whose personal information is breached. This would be a departure from the current Connecticut data breach notification requirements.

Furthermore, the Connecticut data breach notification law has a succinct definition of personal information and defines it as: "an individual's first name or first initial and last name in combination with any one, or more, of the following data: (1) Social Security number; (2) driver's license number or state identification card number; or (3) account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account."[15] As discussed above, the Insurance Requirements only provide broad guidance with regard to the type of personal information that triggers reporting to the Commissioner.

[12] Bulletin IC-25 at 3.

[13] *Id.* at 4.

[14] Conn. Gen. Stat. § 36a-701b(a).

[15] *Id.*

It is also not clear if there will be any accommodations made for delayed reporting under the insurance mandate. The CT data breach notification law makes allowances for delaying notification if a law enforcement agency believes such notice would impede a criminal investigation.[16] The Insurance Requirements do not provide for any delay in reporting or notification to the Commissioner.

Unlike many other state's data breach notification laws, the Connecticut data breach notification law does not require reporting to the Connecticut Department of Consumer Affairs or state Attorney General. This mandate by the Insurance Commissioner may be an attempt to fill that gap.

Insurance Requirements vs. HITECH Act

Many of the Regulated Entities that are covered by the Insurance Requirements would also be subject to HIPAA, and many of their vendors/business associates would be Business Associates under HIPAA, so it also makes sense to compare the obligations under both regimes. Both sets of regulations apply to electronic or paper based data, although the HITECH Act regulations also state that they cover oral disclosures. As with the CT data breach notification law, the HITECH Act defines a breach as the disclosure of "unsecured" (i.e., unencrypted) personal information, while the Insurance Requirements require notice when the consumer is "at risk," regardless of whether the information is encrypted.

The most significant difference is the timing of notice, where HIPAA gives a Covered Entity or a Business Associate up to 60 days to report a breach, the Insurance Requirements require notice to the Insurance Commissioner within five days. That means a Business Associate must notify the Regulated Entity with enough time for the Regulated Entity to meet the 5-day deadline.

Appendix 1 provides a comparison of the requirements under the Insurance Requirements, Connecticut's data breach notification law and HIPAA as modified by the HITECH Act.

Significance

Connecticut is the first state to impose an additional notice requirement to the state insurance commissioner in the wake of a data breach. The Department's actions appear to be consumer protection oriented but it is not clear why the Commissioner could not rely on Connecticut's data breach notification law or other applicable data protection statutes. Interestingly, most of the organizations affected by this mandate must also already comply with HIPAA/HITECH, but the new Connecticut requirements differ from the data breach notification requirements under that law.

There many be instances where the Connecticut Department of Insurance must be notified of a breach but disclosure to the Regulated Entity's customers and/or the Secretary of HHS is not necessary under the state's data breach notification law or HIPAA, respectively. For example, if encrypted data, or even unencrypted paper-based data, is disclosed, reporting to the Commissioner is necessary under the Insurance Requirements but no action is required under the Connecticut data protection law or under HIPAA (provided that the encryption satisfies the HITECH Act regulations).

It is not clear what the Connecticut Insurance Department is going to do with the information collected as part of these mandated disclosures including whether the notices from Regulated Entities will be public information and whether it will be coordinating with the Connecticut Department of Consumer Protection, the U.S. Dept. of Health and Human Services or the FTC.

[16] *Id.* at § 36a-701b(d).

All entities registered with the Connecticut Insurance Department should be aware of this new requirement and update their data breach notification policies and procedures to include these reporting requirements to the Commissioner. Additionally, Regulated Entities that have relationships with third party vendors and business associates should validate that the agreements in place with these organizations provide adequate protections for the Regulated Entity to provide the Connecticut Insurance Department with the information they request and to indemnify against fines levied against the Regulated Entity.

For assistance with regard to data breach notification compliance or for further information, please contact:.

John L. Nicholson (bio)
Washington, DC
+1.202.663.8269
john.nicholson@pillsburylaw.com

Meighan E. O'Reardon (bio)
Washington, DC
+1.202.663.8377
meighan.oreardon@pillsburylaw.com

Appendix 1

Requirement	Insurance Requirements	CT Data Breach Notification Law	HITECH Act
Entities Covered	All licensees and registrants of the Connecticut Insurance Department	Any person who conducts business in CT, and who, in the ordinary course of such person's business, owns, licenses or maintains computerized data that includes personal information	HIPAA Covered Entities
Definition of Personal Information	Personal health, financial or personal information" (at least 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.)	Individual's first name or first initial and last name in combination with any one, or more, of the following data: (1) Social Security number; (2) driver's license number or state identification card number; or (3) account number, credit or debit card number, in combination with any required security code, access code or password that would permit access to an individual's financial account	Protected health information (PHI) under HIPAA includes any individually identifiable health information
Data Format	In whatever format the data is collected, used or stored	Electronic files, media, databases or computerized data	Electronic data as well as data transmitted or maintained in any other form or medium including paper records, fax documents and oral communications
Encrypted vs. Unencrypted	Both	Unencrypted	Unencrypted (unsecured protected health information (information that has not been rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in guidance))

Requirement	Insurance Requirements	CT Data Breach Notification Law	HITECH Act
Definition of Breach	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, policy holder 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	Unauthorized access to or acquisition of electronic files, media, databases or computerized data containing personal information when access to the personal information has not been secured by encryption or by any other method or technology that renders the personal information unreadable or unusable	Impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information
Standard for Notice	Breach could compromise or put at risk the personal, financial, or physical well being of the affected insureds, members, subscribers, policyholders or providers	Notification shall not be required if, after an appropriate investigation and consultation with relevant federal, state and local agencies responsible for law enforcement, the person reasonably determines that the breach will not likely result in harm to the individuals whose personal information has been acquired and accessed	Use or disclosure poses a significant risk of financial, reputational, or other harm to the affected individual; EXCEPT ▪ unintentional acquisition, access, or use of PHI by a workforce member acting under the authority of a covered entity or business associate ▪ inadvertent disclosure of PHI from a person authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the covered entity or business associate ▪ if the covered entity or business associate has a good faith belief that the unauthorized individual, to whom the impermissible disclosure was made, would not have been able to retain the information

Requirement	Insurance Requirements	CT Data Breach Notification Law	HITECH Act
Notice Timing	As soon as the incident is identified but not later than five calendar days after the incident is identified	Without unreasonable delay	▪ Individuals without unreasonable delay and in no case later than 60 days following the discovery of a breach ▪ For breach affecting >500 individuals, must notify the Secretary of HHS without unreasonable delay and in no case later than 60 days following a breach ▪ For breach affecting < 500 individuals, the covered entity may notify the Secretary of such breaches on an annual basis (within 60 days of end of calendar year)
Law Enforcement Exception	None	Any notification required by this section shall be delayed for a reasonable period of time if a law enforcement agency determines that the notification will impede a criminal investigation and such law enforcement agency has made a request that the notification be delayed. Any such delayed notification shall be made after such law enforcement agency determines that notification will not compromise the criminal investigation and so notifies the person of such determination.	None
Notice To	CT Insurance Commissioner	Affected Consumer	Affected Individuals' Secretary of HHS
Credit Monitoring Required	Possible	None	None

Requirement	Insurance Requirements	CT Data Breach Notification Law	HITECH Act
Other Penalties	Possible	Failure to comply with the requirements of this section shall constitute an unfair trade practice for purposes of section 42-110b and shall be enforced by the Attorney General.	▪ four categories of violations that reflect increasing levels of culpability; ▪ four corresponding tiers of penalty amounts that significantly increase the minimum penalty amount for each violation; and ▪ maximum penalty amount of $1.5 million for all violations of an identical provision.