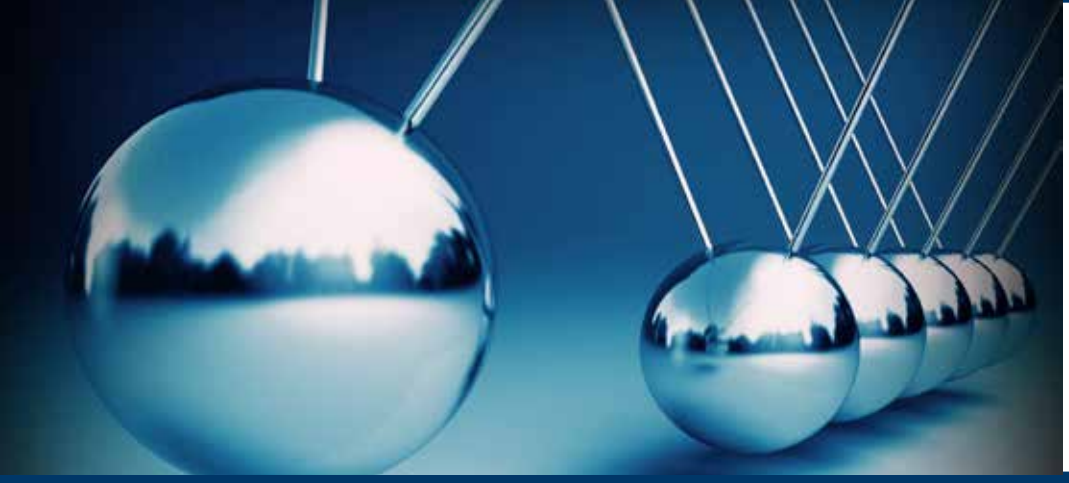

MURTHA MEANS
# MORE
INDUSTRY INSIGHT

## INFORMATION SECURITY AND PRIVACY GROUP NEWS

June 2015

### CONNECTICUT'S DATA SECURITY LAW EXPANDS

Anyone that conducts business in Connecticut is required by law to report any "data security breach"[1] to the Attorney General and to affected customers who are Connecticut residents. This June, the Legislature added some meat to this pre-existing law.[2] The new bill, S.B. 949 (the "Act" or "law"), contains three main requirements. First, it requires that any individual, business, or other entity that receives confidential information from any "State contracting agency"—pursuant to a written agreement with that agency to provide goods or services to the state—implement a data-security program by July 1, 2015. Second, it requires that any health insurer, health care center, pharmacy benefits manager, third-party administrator, utilization review company, or other entity licensed to do health insurance business in Connecticut, implement an information security program by July 1, 2017. Third, it requires anyone doing business in Connecticut to notify Connecticut residents whose personal information was breached and the Attorney General's office within 90 days of discovering a breach and to provide free identity-theft services for one year to persons whose information was accessed during a breach.

This law demonstrates another example of the continued expansion of data-security law throughout the United States. Here, the Connecticut legislature has specifically targeted businesses and individuals that receive confidential information from a State agency and that conduct business in the health insurance industry. However, it is important to realize that the State's pre-existing data security law, as amended by S.B. 949, affects any person who conducts business in Connecticut. Further, Connecticut's data security laws represent only a sliver of the state and federal laws that could apply to you regarding the information you maintain. Therefore, it would be wise to implement a data-security program regardless of who you are. Failing to do so could result in million-dollar judgments, hefty fines, and lawsuits brought by the state and federal government.

#### If You Receive Individuals' Confidential Information Under a Written Agreement With a State Contracting Agency Then You Must Implement a Data-Security Program.

In addition to having to report any data security breaches, S.B. 949 requires certain businesses and

[1] A "data security breach" occurs when an unauthorized person or entity gains access to an individual's "personal information" (e.g. a Social Security number, driver's license number, or bank account number). "Personal information" means a person's first and last name (or first initial and last name) plus some other information of theirs, such as a Social Security number, credit card number, etc.

[2] At the time of press, this bill is awaiting the Governor's signature.


If you have any questions about the issues addressed here, or any other matters involving Information Security and Privacy issues, please feel free to contact:

Burt Cohen, Chair
bcohen@murthalaw.com

Susan J. Baronoff
sbaronoff@murthalaw.com

Heather O. Berchem
hberchem@murthalaw.com

Stella Szantova Giordano
sgiordano@murthalaw.com

Rachel Snow Kindseth
rkindseth@murthalaw.com

James F. Radke
jradke@murthalaw.com

Stephanie Sprague Sobkowiak
ssobkowiak@murthalaw.com

Edward B. Whittemore
ewhittemore@murthalaw.com

individuals, beginning July 1, 2015, to implement and maintain data security programs to protect confidential information. This law applies to any individual business, or other entity that has a written agreement with a Connecticut State agency to provide goods and services to that agency and, in the course of doing that work, receives "confidential information" from the State. "Confidential information" means information capable of being associated with a particular individual through one or more identifiers, including, but not limited to, the following:

- A person's name
- Date of birth
- Mother's maiden name
- Motor vehicle operator's license number
- Social Security number
- Employee identification number
- Employer or taxpayer identification number
- Alien registration number
- Government passport number
- Health insurance identification number
- Demand deposit account number
- Savings account number
- Credit card number
- Debit card number
- Fingerprints, voice prints, retina or iris images

In addition to the laundry list above, any information that a State agency identifies as "confidential" falls under this definition as well. Therefore, if you are an individual or business and you (1) have a contract with a State agency and (2) you receive from that State agency any of the above information, then you must comply with this new law.

The Act requires these individuals and businesses to enact policies to prevent data security breaches. These policies must, at the minimum, restrict access to confidential information only to appropriate persons, be annually reviewed, include ongoing employee training, and maintain the confidential information in secure servers with firewall protections.

The Act also creates numerous restrictions on how you can use the data you receive from state agencies. For example, it makes clear that you can no longer store confidential information on portable storage devices, such as USB drives. Among other prohibitions, it prohibits copying, reproducing, or transmitting confidential information unless you need to do so for a business purpose.

Any violators of this Act could be subject to a lawsuit filed by the Attorney General of Connecticut.[3] Because the Act presents further regulations for certain businesses, these businesses should be diligent in creating a practical and workable data-security policy. It is important to recognize that the Act applies to any individual, business, or other entity that receives confidential information from a Connecticut state agency pursuant to a written agreement with that agency to provide goods or services to the state. In other words, companies of all sizes and individuals, regardless of which State they are located in, could be subject to this law.

[3] If your business maintains confidential information specifically relating to education records, a data security breach could result in a 5-year ban of receiving that information from the State Department of Education.

The Act says the effective date of these provisions is July 1, 2015. Our firm has confirmed with officials at the Connecticut Office of Policy and Management (OPM) that the requirements of Sections 1 and 2 of the Act will only apply to new written agreements, and extensions of or amendments to existing agreements, between a contractor and a State contracting agency that are entered into or become effective on or after July 1, 2015. Presumably, OPM will instruct state agencies that existing agreements will also become covered by the law after July 1, 2015, but only upon the renewal, amendment or extension of any such agreements.

### The Office of Policy and Management to Oversee the State's Data

The Act also requires the OPM, beginning July 1, 2015, to develop a large program designed to link all data maintained by executive agencies. This program may take some time to set into action, but its purpose is to make it easier and safer for State agencies to maintain persons' confidential information.

Although this part of the Act probably will not have much effect on private businesses, it may promote easier access. In particular, the Act allows for businesses, companies, or individuals, to send formal requests to the OPM for data maintained by two or more executive agencies. However, in order to make such a request, you must require access to such data as a part of your business or operation. Private companies like this should be aware that the Act gives priority to requests made by State agencies that use the data to measure outcomes of state-funded programs.

The Act also gives the OPM the authority to require companies or businesses to implement additional measures of protection. The OPM may do this at its discretion if it finds that circumstances warrant such action.

### Entities Licensed to do Health Insurance Business in Connecticut Must Implement Privacy Policies

By October 1, 2017, any health insurer, health care center, pharmacy benefits manager, third-party administrator, utilization review company, or entity that is licensed to do health insurance business in Connecticut must implement and maintain a data security program. In addition, such entities must annually certify, beginning October 1, 2017, to the Insurance Department, that they have implemented a data security program. The purpose of this requirement is to protect the "personal information" of insureds. At the minimum, the security program must:

- Protect personal information
- Restrict access to personal information
- Maintain secure password-protected computers and devices
- Encrypt certain stored data
- Continually monitor the security system
- Keep up-to-date security software
- Ongoing education and training of employees
- Designate one or more employees to oversee the program
- Identify and assess security risks
- Impose disciplinary measures for employees who violating security policies
- Oversee third parties that have access to the company's data
- Restrict physical access to paper-format data
- Review the program at least annually
- Investigate and review any actual or suspected breach of security

For companies licensed to conduct health-insurance business in Connecticut, the Insurance Commissioner will enforce this part of the Act. However, the Act also incorporates the pre-existing penalties of Connecticut's data-security breach law. Thus, if you are subject to this law, and violate it, you could be sued by private individuals for an Unfair Trade Practice or by the Attorney General.[4]

### Any Person Who Conducts Business in Connecticut Must Report Breaches within 90 Days of Discovery and Provide Free Identity Theft Services for One Year

Under existing data security law in Connecticut, any person conducting business in Connecticut is required to report any data breach to customers who are Connecticut residents whose information was accessed during the breach and to the Attorney General. Initially, the law never specified how much time is allotted to notify residents, other than to require that the notice "be made without unreasonable delay." Now it does. Starting October 1, 2015, any person conducting business in Connecticut that experiences a data breach has 90 days after the discovery of the breach to notify affected Connecticut residents, unless a shorter time is required under federal law or if waiting 90 days to provide notice would constitute "unreasonable delay."

In addition to specifying a time limit, the Act now requires those who experience a data breach to provide free identity-theft services (and in some cases identity-theft mitigation services) to customers who are Connecticut residents. These services must be provided, at no cost to the resident, for at least one year. The office of the Connecticut Attorney General has indicated that it will continue to seek two years of appropriate identity theft services when the Attorney General deems it necessary to protect Connecticut residents. If a data-security breach is big enough, this could have an adverse financial impact on any business operation or individual. The Legislature likely wants to incentivize companies to create efficient and secure data-privacy policies. Therefore, devoting the resources, up front, toward ensuring that your data-privacy policy is legally sound could be a saving grace down the road.

### Sellers of Smartphones Must Ensure That Phones Are Secure

Starting July 1, 2016, and until July 1, 2017, no person can offer for sale at retail a smartphone, in Connecticut, unless the smartphone includes software or hardware that prevents unauthorized users from accessing the phone's essential features.

*If you have any questions about the Act and its impact on your business, please contact your Murtha Cullina attorney or Burt Cohen at bcohen@murthalaw.com or 203-772-7714.*

---

[4] This part of the Act (that applies to entities in the health-insurance industry) is much harsher than the part of the Act (discussed above) that only applies to those doing business with State agencies. Unlike that provision, which contains no private right of action, the provision applying to health insurers does.