MINTZ

State Data Breach Notification Law Updates

March 10, 2015 | Blog | By **Cynthia J. Larose**

VIEWPOINT TOPICS

- Privacy & Cybersecurity

RELATED PRACTICES

RELATED INDUSTRIES

State legislatures are not waiting for Congressional action on a national data breach notification standard.

Montana -- Montana has amended its 10-year old breach notification law (see **Mintz Matrix**) to expand the definition of "personal information" and require notice to the state attorney general's consumer protection office. *H.B. 74*, signed into law by Governor Bullock, adds medical record information and **"identity protection personal identification number" issued by the Internal Revenue Service** to the definition of "personal information." The amended statute takes effect October 1.

New Jersey -- Governor Christie recently signed legislation into law requiring health insurance companies in that state to encrypt personal information of policyholders. All health insurance carriers that compile computer records that contain personal information must protect those records through encryption or "by any other method or technology rendering it unreadable, undecipherable, or otherwise unusable by an unauthorized person." **In November 2013, two laptops with unencrypted information about 840,000 policyholders** were stolen from an office at Horizon Blue Cross Blue Shield of New Jersey in Newark. The Barnabas Health Medical Group's Pediatric branch in Livingston and the Inspira Medical Center in Vineland also had breaches in 2013, **according to a NJ Advance Media report in September.**

Connecticut -- In the aftermath of the massive **Anthem data breach**, legislation has been introduced in the Connecticut General Assembly requiring a wide swath of insurance businesses to implement data security technology that encrypts personal information of insureds. The covered entities include health insurers, healthcare centers – similar to an HMO under Connecticut's insurance laws, and "other entities licensed to do health insurance business in Connecticut," pharmacy benefits managers, third-party administrators that administer health benefits, and utilization review companies. The requirement is similar to that of New Jersey's new law, except that the bill requires that entities subject to the law update their technology as necessary to ensure compliance. Anthem is one of Connecticut's largest health insurers, and reportedly that breach impacted more than 1 million people in the state. See **"Act Concerning the Security of Consumer Data"**.

Washington -- The Washington House has unanimously passed a bill that would make the failure to notify consumers of a breach as required by the state's data breach notification law (again, see the **Mintz Matrix**) a violation of the state's Consumer Protection Act. Washington's House of Representatives has passed a bill (**H.B. 1078**) that would make the failure to notify consumers of a breach in the security of their personal information a violation of the state Consumer Protection Act. The measure would require notification to consumers -- and the state's AG -- as quickly as possible and no later than 45 days after discovery of a breach of personal information such as a person's name in combination with a Social Security number, driver's license number or payment card number and payment card access code or password. Under the bill, the attorney general could bring an action on behalf of the state or consumers living in Washington.

New Mexico -- New Mexico is only one of three holdouts from the state data breach notification crazy quilt (again, see the **Mintz Matrix**), but HB 217, the **Data Breach Notification Act**, is working its way through the state legislature. The bill only applies to computerized data, and uses an "acquisition" trigger for breach notification. "Personal information" under HB 217 is defined as the "usual suspects" and does not include username/password or other login credentials. The bill requires "reasonable security" and includes disposal provisions that apply to paper records as well as electronic. Similar legislation failed in the 2014 session of the legislation, thus it remains to be seen whether New Mexico will join the **Mintz Matrix** this year.

Authors

Cynthia J. Larose, Member / Co-chair, Privacy & Cybersecurity Practice

Cynthia J. Larose is Chair of the firm's Privacy & Cybersecurity Practice, a Certified Information Privacy Professional-US (CIPP-US), and a Certified Information Privacy Professional-Europe (CIPP-E). She works with clients in various industries to develop comprehensive information security programs on the front end, and provides timely counsel when it becomes necessary to respond to a data breach.