Alabama Legislature Considers State Law on Cybersecurity

By Jim Hoover and Angie C. Smith April 2018

Reprinted with Permission from the *Birmingham Medical News*

At the time of the writing of this article, Alabama is one step closer to having a law on the books related to cybersecurity. Alabama is currently one of two states along with South Dakota that have not passed a data breach notification law. The legislation Alabama is considering requires certain entities defined as "covered entities," to report to state agencies and affected individuals when there has been an unauthorized acquisition of "electronic, sensitive personally identifying information."

On March 1, 2018, the Alabama Senate passed SB318, and if passed by the House and signed by the Governor, it would require "covered entities" to notify Alabama's attorney general, Alabama residents whose information has been compromised, and consumer credit-reporting agencies of a data breach. For healthcare providers covered by the Health Insurance Portability and Accountability Act ("HIPAA"), federal law already requires notification when they experience unauthorized disclosures of protected health information. In addition to HIPAA's breach notification requirements, the new Alabama law would require reporting at the state level for healthcare providers who experience a data breach. It is important to note that the term "covered entities" in the proposed legislation is much broader than HIPAA's definition of "covered entity." The term in SB318 applies to persons or business entities that acquire or use personally identifiable information.

Under SB318, a covered entity is required to investigate any data breach and in some instances report the breach. The investigation must include (1) an assessment of the nature and scope of the breach, (2) identification of any sensitive personally identifying information involved and the individuals involved, (3) a determination as to whether the information was acquired by an unauthorized individual and could result in substantial harm, and (4) identification and implementation of measures to restore security and confidentiality of the system involved in the breach. When determining if a breach is reportable, a determination must be made whether sensitive information is reasonably believed to have been acquired by an unauthorized person, and whether the unauthorized acquisition is reasonably likely to cause substantial harm to the individuals.

SB318 sets forth four factors to consider when evaluating whether the information is "reasonably believed" to have been acquired by an unauthorized individual. In making this determination, the covered entity must evaluate "indications that the information is in the physical possession and control of a person without valid authorization, such as a lost or stolen computer or other device containing information; indications that the information has been downloaded or copied; indications that the information was used by an unauthorized person, such as fraudulent accounts opened or instances of identity theft reported; and whether the information has been made public." The law however does not provide guidance on whether the breach is reasonably likely to cause substantial harm to the affected individual.

Even if a breach is not a reportable event, the covered entity must maintain relevant records for at least five years. For instance, if the covered entity determines the breach is not reasonably likely to cause substantial harm then no notification is required, but the entity must keep all records related to the breach and their determination that notification was not necessary for five years following the incident.

SB318 also requires covered entities to implement "reasonable security measures" to protect an individual's data. Similar to HIPAA, the bill requires the covered entity to designate an employee to coordinate security measures (i.e. Security Officer) and to identify risks of data breaches. In recognizing that not all covered entities face the same risks or have the same resources, the required "reasonable" security measures should take into account the size of the covered entity, the amount of data maintained and stored by the covered entity and the cost to implement security measures. Good news for healthcare providers, if a healthcare provider has performed the necessary security and risk assessments required under HIPAA, it should meet the standards required in SB318.

Not all information qualifies as "sensitive personally identifiable information." To meet this definition, the accessed information must consist of the individual's first name or initial and last name in combination with any one of the following data elements: a non-truncated (or shortened) Social Security or tax identification number; non-truncated driver's license, state-issued identification card number, passport number, military identification number or any unique, government-issued number used to verify identity; a financial account, credit or debit card number along with a required security code, expiration date, PIN, access code or password necessary to access a financial account or conduct a transaction; individual medical or mental history or treatment information; a health insurance policy or identification number; or a user name or email address along with a password or security question and answer that gives access to an online account that is likely to contain sensitive personal information.

If notification must be made, the covered entity must provide notification as "expeditiously as possible" but no more than 45 days after the determination of the breach. The notification may be made by mail or email and must include the following elements: the date, estimated date, or estimated date range of the breach; a description of the sensitive personally identifying information that was acquired by an unauthorized person as part of the breach; a general description of the actions taken by a covered entity to restore the security and confidentiality of the personal information involved in the breach; a general description of steps a consumer can take to protect himself or herself from identity theft; and information that the individual can use to contact the covered entity to inquire about the breach.

A violation of SB318 constitutes a deceptive trade practice, but does not constitute a criminal offense. The attorney general may seek deceptive trade practice penalties when a covered entity or third-party agent knowingly violates the notification law. The Deceptive Trade Practice Act penalties would apply for willful or reckless disregard of the notification requirements that could subject the violator to a $2,000-per-person penalty, capped at $500,000. Any entity that made notification after the 45-day deadline could also be fined up to $5,000 per day.

The bill is currently pending before the Alabama House of Representatives, bill number HB410.

For more information, please contact:

Jim Hoover
Partner
Birmingham, AL
Phone (205) 458-5111
E-Mail jhoover@burr.com

Jim Hoover is a partner in Burr & Forman's Health Care Practice Group in Birmingham and exclusively represents health care providers in false claims litigation and regulatory compliance matters.

Angie C. Smith
Partner
Birmingham, AL
Phone (205) 458-5209
E-Mail acsmith@burr.com

Angie C. Smith is a partner in Burr & Forman's Health Care Practice Group in Birmingham.