BURR FORMAN LLP

Alabama Legislature Considers State Law on Cybersecurity

Articles / Publications
04.09.2018

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.

RELATED PROFESSIONALS

James A. Hoover

Angie Cameron Smith

Alabama Legislature Considers State Law on Cybersecurity

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.

Download the full article, "Alabama Legislature Considers State Law on Cybersecurity" written by Jim Hoover and Angie C. Smith.

Related Article

Medical Association of the State of Alabama: Alabama Legislature Considers State Law on Cybersecurity (Angie C. Smith)