Following on the heels of an active 2015, where eight states enacted changes to their data breach notification laws, another five states amended their statutes in 2016, adding complexity to the current “patchwork” system of breach notification legislation. Several trends have emerged from these recent enactments. States are broadening the definition of “personal information,” redefining content and timing requirements for notification, clarifying the role of encryption in providing a safe harbor, and providing carveouts for entities compliant with other privacy regulations.
The amendments enacted in Nebraska, Tennessee, and Arizona all took effect in 2016, while the updates in California and Illinois became effective on January 1, 2017. For a summary of the amendments, please click on the image below.

The divergent and frequently changing state statutes create challenges for compliance and may require organizations to revisit their security incident response plans and other privacy policies and procedures to ensure that the policies reflect these new obligations.

Next Steps

As states continue to revise their data breach laws, organizations must continue to monitor these changes to prepare for and respond to data breaches.

- In particular, because of the expansions to what constitutes “personal information,” companies must continue to conduct assessments of the information they collect and receive, and create data maps to have a better understanding of their data in order to implement appropriate procedural and security safeguards.

- Organizations should also review security measures to ensure that an incident involving encrypted data does not go undetected.

- Organizations also need to understand if they are required to comply with GLBA or HIPAA and how those laws affect compliance with state data breach laws.

© 2020 Foley & Lardner LLP