Update on Colorado's Proposed Privacy and Cybersecurity Legislation

By David M. Stauss and Gregory Szewczyk*

The Colorado legislature is considering legislation that, if enacted, would significantly change Colorado privacy and data security law. This article discusses the most significant changes.

The Colorado legislature is considering legislation that, if enacted, would significantly change Colorado privacy and data security law. The bill's sponsors submitted an amended bill[1] that addresses issues raised by numerous stakeholders. The amended bill also was heard before the House Committee on State, Veterans, and Military Affairs, where it was unanimously approved. The most significant changes are highlighted below.

PROPOSED DATA DISPOSAL AND SECURITY REQUIREMENTS

The bill would create a new statute, C.R.S. 6-1-713.5, that would require entities to implement and maintain "reasonable security procedures and practices" to protect "personal identifying information" ("PII") of Colorado residents. The bill also would amend C.R.S. 6-1-713 to require entities to develop a written policy for the destruction or proper disposal of paper or electronic documents that contain PII.

The amended bill adds new language to each of those statutes, stating that any entity regulated by state or federal law and that maintains procedures for disposal and protection of PII pursuant to the "laws, rules, regulations, or guidances or guidelines established by its state or federal regulator is in compliance" with the amended bill's data disposal and security requirements.

This revision was intended to address concerns raised by entities subject to HIPAA's Security Rule[2] and the Gramm-Leach-Bliley Act ("GLBA") Safeguards Rule.[3]

---

* David M. Stauss is a partner at Ballard Spahr LLP and head of the Denver office's Privacy and Cybersecurity Practice Group. Gregory Szewczyk is an associate at the firm handling corporate and commercial litigation, as well as privacy and cybersecurity matters. The authors may be reached at staussd@ballardspahr.com and szewczykg@ballardspahr.com, respectively.

[1] https://leg.colorado.gov/sites/default/files/documents/2018a/bills/cr/2018a_hb1128_h_sa_001.pdf.

[2] https://www.hhs.gov/hipaa/for-professionals/security/index.html.

[3] https://www.ecfr.gov/cgi-bin/text-idx?c=ecfr&sid=1e9a81d52a0904d70a046d0675d613b0&rgn=div5&view=text&node=16%3A1.0.1.3.38&idno=16.

Specifically, under HIPAA's Security Rule, health plans, health care clearinghouses, and some health care providers are required to implement appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. Similarly, GLBA's Safeguards Rule requires financial institutions to "develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to [their] size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue."

However, this new provision will only create a partial safe harbor for HIPAA/GLBA-regulated entities because the Colorado statute's definition of "personal identifying information" is different than the definitions of "electronic protected health information" and "customer information" under the Security and Safeguards Rules. For example, while GLBA focuses on "customer information," the Colorado statute's definition of PII would extend to the confidential information of employees. Further, with respect to HIPAA, the Colorado statute's definition of PII does not include health or medical information but does include other types of information that are beyond HIPAA's coverage, such as passwords and passcodes.

The takeaway is that while this new language will help HIPAA/GLBA-regulated entities, they will still need to take measures to ensure compliance with the Colorado statute.

PROPOSED CHANGES TO COLORADO'S BREACH NOTIFICATION LAW

Expanded Definition of Personal Information

The initial bill expanded the categories of "personal information" that are covered by the data breach notification. At the hearing, the committee adopted an amendment to further expand the definition of "personal information" to include student, military, or passport identification numbers.

Proposed Changes Regarding Breach Notification Timing

The amended bill substantially revises the proposed notification time requirements. Under current Colorado law, entities must provide notice to affected individuals "in the most expedient time possible and without unreasonable delay." The initial draft bill changed that provision to require that notice be provided no later than 45 days "from the date of the security breach." That language created concerns because entities often do not know that there has been a loss or compromise of confidential information until well after the security breach.

The amended bill provides that notice must be provided "not later than 30 days after the date of determination that a security breach occurred." The amended bill also defines "determination that the security breach occurred" as "the point in time at which there is sufficient evidence to conclude that a security breach has taken place."

If the amended bill passes as currently written, Colorado would join Florida as the two states with the strictest time period for providing notice. However, Colorado would be even stricter than Florida, because Florida's statute allows for an additional 15 days to provide notice "if good cause for the delay is provided to the [Florida Department of Legal Affairs] within 30 days after determination of the breach or reason to believe a breach occurred." North Carolina is considering legislation that would require notice to be provided in 15 days.

The amended bill also addresses how Colorado's 30-day notice time period interacts with HIPAA's 60-day notice time period under its Breach Notification Rule.[4] This issue arose because the Colorado bill adds medical information and health insurance identification numbers to the types of "personal information" covered by the statute, thereby creating an overlap with HIPAA's definition of personal health information. The amended bill states that "in the case of a conflict between the time period for notice to individuals [under Colorado law and a state or federal regulator's law or regulation] the law or regulation with the shortest time frame for notice to the individual controls."

That provision was the subject of extensive testimony at the Committee hearing and it is expected that the language will receive further consideration as the bill moves forward.

Proposed Changes Regarding Alternative Notification

The amended bill also creates an alternative means of notification for breaches involving a Colorado resident's username or email address. In those instances, an entity can notify individuals in an electronic or other form that directs them to change their passwords, security questions, and answers for their accounts and for any other accounts where they use the same login information. However, that notification must be provided "no later than five days after the determination that a security breach occurred."

Proposed Changes Regarding Notice to the Attorney General's Office

The amended bill also changes the time frame for notifying the Attorney General's office of a security event involving 500 or more Colorado residents. As originally proposed, entities would have been required to notify the Attorney General's office

[4] https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html.

within seven days after discovery of the breach. The amended bill significantly expands that time frame to 30 days. It also clarifies that notice does not need to be provided if "the investigation determines that the misuse of information about a Colorado resident has not occurred and is not likely to occur." Finally, the amended bill adds new provisions that create similar obligations for government entities. This would be the first time that Colorado law requires government entities to notify affected individuals of a security event as the existing law excludes government entities by defining "commercial entity" as "any private legal entity."