Nevada and New Hampshire Add Data Security and Privacy Laws

DANA B. ROSENFELD AND KRISTIN A. HIRD

In this article, the authors discuss the key provisions of new privacy and data security laws that took effect recently in both Nevada and New Hampshire.

New privacy and data security laws took effect in Nevada and New Hampshire on January 1, 2010, continuing the trend of state governments acting to strengthen data security laws. Nevada's law makes it the first state to mandate compliance with the entire Payment Card Industry Data Security Standard ("PCI DSS") and impose a requirement on businesses and government agencies to encrypt sensitive data transmitted or carried outside of the premises of the business or agency. New Hampshire's law first sets forth restrictions regarding the use and disclosure of personal health information for marketing or fundraising purposes and then sets forth a disclosure requirement if there is unauthorized use or disclosure of protected health information in violation of New Hampshire law, even if the use or disclosure is allowed under federal law.

Dana B. Rosenfeld and Kristin A. Hird are attorneys in the Advertising and Marketing practice at Kelley Drye & Warren LLP in Washington, D.C. Ms. Rosenfeld is a partner and chair of the Privacy and Information Security practice group, and Ms. Hird is an associate. The authors can be reached at drosenfeld@kelleydrye.com and khird@kelleydrye.com, respectively.

Published in the January 2010 issue of Privacy & Data Security Law Journal.

NEVADA LAW

Nevada's law addresses transaction data created by a customer's use of a credit, debit, or other payment card, and personal information, and applies to "a data collector doing business" in Nevada. While the question of what constitutes "doing business" in a state requires a fact-specific analysis, the Nevada law is clear in its adoption of PCI DSS standards. Specifically, a data collector that accepts payment cards is now required to comply with "the current version" of the PCI DSS, no later than the date for compliance set forth by the PCI DSS or the PCI Security Standards Council. Data collectors who do not accept payment cards must use encryption when transferring personal information through "an electronic, nonvoice transmission other than a facsimile" to a person outside the secure system of the data collector and when moving any data storage device containing personal information "beyond the logical or physical controls of the data collector." By enacting this law, Nevada essentially codifies the PCI DSS standards.

New Definition of Encryption

The Nevada law also repeals a prior statute that defined the term "encryption" more flexibly. The new law defines "encryption" as (1) "an encryption technology that has been adopted by an established standards setting body, including, but not limited to, the Federal Information Processing Standards issued by the National Institute of Standards and Technology" and (2) "[a]ppropriate management and safeguards of cryptographic keys to protect the integrity of the encryption using guidelines promulgated by an established standards setting body, including, but not limited to, the National Institute of Standards and Technology." Whereas the prior statutory definition of encryption permitted use of a wide range of technologies as long as the essential purpose of protection was accomplished, the new law now defines which technologies are acceptable.

Safe Harbor

The new law establishes a safe harbor by stating that a data collector is not liable for damages for a breach of the system data security if the

data collector is in compliance with this law and the security breach is not caused by the gross negligence or intentional misconduct of the data collector, its officers, employees, or agents. The new law, however, does not identify a party empowered to enforce the statute nor does it specifically create an individual cause of action. Likewise, the law does not specify penalties or remedies for noncompliance. Since the new law resides in the Trade Regulations and Practices title, which generally grants the state Attorney General enforcement authority, it is likely that the Nevada Attorney General will be able to seek an injunction, restitution, or monetary relief for its citizens based on harms resulting from a violation.

NEW HAMPSHIRE LAW

New Hampshire's new medical records and patient information law sets forth requirements for the use of health care information for marketing and fundraising purposes and mandates that health care providers and business associates notify individuals in writing upon the unauthorized use or disclosure of their protected health information if such uses or disclosures violate New Hampshire law, even if such disclosures are "allowed under federal law." Importantly, unlike New Hampshire's general data breach notification law, there is no risk of harm threshold that must be met to trigger the notification requirement.[1]

Definition of Health Care Provider

The data breach notification law applies to health care information in the possession of health care providers and business associates of health care providers. While the law adopts definitions in the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") for the terms "business associate," "use," "disclosure," and "protected health information," it sets forth its own definition of "health care provider." The law establishes a broad definition, defining the term as "any person, corporation, facility, or institution either licensed by this state or otherwise lawfully providing health care services, including, but not limited to, a physician, hospital, office, clinic, health center or other health care facility, dentist, nurse, optometrist, pharmacist, podiatrist, physical therapist, or mental health pro-

fessional, and any officer, employee, or agent of such provider acting in the course and scope of employment or agency related to or supportive of health care services."

Marketing and Fundraising

The law requires health care providers and business associates to obtain authorization for any use or disclosure of protected health information ("PHI") for marketing purposes. The authorization must meet the implementation specifications for marketing adopted in Sections 262 and 264 of HIPAA, as amended. The New Hampshire law defines marketing as "a communication about a product or service that encourages recipients of the communication to purchase or use the product or service," except for communications made by the individual's health care provider to the individual for treatment, case management, care coordination, and other related activities. Marketing is also defined as an arrangement in which a health care provider discloses PHI in exchange for direct or indirect remuneration, so that the other person may "make a communication about the person's own product or service that encourages recipients of the communication to purchase or use that product or service."

Individuals must also be provided with an opt-out prior to the use and disclosure of the PHI for fundraising purposes and that opt-out must be provided in a "clear and conspicuous manner," which includes simple election language and easily readable type. This notice must be provided sixty days before the fundraising communication, on presentation of a notice of privacy practices distributed under HIPAA and given before the fundraising communication, or in a later fundraising communication if the individual did not opt-out earlier.

For either marketing or fundraising, PHI must not be disclosed by voice mail, unattended facsimile, or "through other means that are not secure."

Notification and Remedies for Disclosure

Under the law, in the event of a use or disclosure of PHI by a health care provider or business associate "that is allowed under federal law but not permitted by RSA 332:1:4 [the marketing and fundraising provision],"

the health care provider or business associate must "promptly" notify the individual or individuals whose PHI was disclosed. The law does not specify the time period for providing notice, nor does it include requirements for the content of the notice. Notably, however, the law does establish an individual cause of action for violations of the new law and mandates significant penalties. Aggrieved individuals may bring action for violations of the new law and damages are specified as "not less than $1,000 for each violation, and costs and reasonable legal fees."

CONCLUSION

Although to date only Minnesota has codified one part of PCI DSS, Nevada's new codification of the entire PCI DSS may well encourage other states to follow its lead in adopting PCI DSS as states did after California enacted the first information security breach notification statute. Even in the absence of new state laws, businesses with a nationwide presence may find themselves operating under a new standard due to the practical difficulty of separating information for Nevada customers from non-Nevada customers. The New Hampshire law, applying only to health care providers and business associates, may have more limited business impact. Nonetheless, it shows that affected companies may not look only to federal law when handling PHI and instead must also consider state laws that, in some cases, extend beyond HIPAA. As such, careful attention to state privacy and data security laws remains a prerequisite for companies handling private customer information.

NOTES

[1] The relevant provision of New Hampshire's data breach notification law, codified at N.H. Rev. Stat. Ann. § 359-C:20(I)(a), states that "[a]ny person doing business in this state who owns or licenses computerized data that includes personal information shall, when it becomes aware of a security breach, promptly determine the likelihood that the information has been or will be misused. If the determination is that misuse of the information has occurred or is reasonably likely to occur, or if a determination cannot be made, the person shall notify the affected individuals as soon as possible as required under this subdivision."

Published in the January 2010 issue of Privacy & Data Security Law Journal.