KING & SPALDING

Client Alert

Healthcare Practice Group

May 12, 2017

New Mexico Enacts Data Breach Notification Law

On April 6, 2017, New Mexico became the 48th state to enact a data breach notification law; the Data Breach Notification Act (the "Act") will go into effect on June 16, 2017.

The good news for many in the health care industry is the Act does not apply to those subject to the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). Financial institutions subject to the Gramm-Leach-Bliley Act are also exempt.

For those to whom the Act applies, including some direct-to-consumer health platforms, medical device manufacturers and pharma companies, the Act imposes certain security and contractual safeguards that are similar to HIPAA. Below is a summary of the Act's key provisions.

Applicability

The Act applies to individuals, corporations, business trusts, estates, trusts, partnerships, limited liability companies, associations, joint ventures and any other legal or commercial entities (collectively referred to as "Persons" defined by NM Stat § 12-2A-3) that own or license elements that include "personal identifying information" of New Mexico residents ("PII").

Information Protected

The Act applies to PII that is not encrypted, sufficiently redacted or otherwise rendered unreadable or unusual. PII is specifically defined to include an individual's first name or first initial and last name in combination with one or more of the following data elements that relate to the individual:

- Social security number;
- Driver's license number;
- Government-issued identification number;
- Account number, credit card number or debit card number in combination with any required security code, access code or password that would permit access to a person's financial account; or
- Biometric data, which is a record generated by automatic measurements of an identified individual's fingerprints, voice print, iris or retina patterns, facial characteristics or hand geometry that is used to

For more information, contact:

Marcia L. Augsburger
+1 916 321 4803
maugsburger@kslaw.com

Lara D. Compton
+ 213 443 4369
lcompton@kslaw.com

R.J. Cooper
+1 916 321 4809
rcooper@kslaw.com

King & Spalding
Los Angeles
633 West Fifth Street
Suite 1700
Los Angeles, CA 90071
Tel: +1 213 443 4355
Fax: +1 213 443 4310

Sacramento
621 Capitol Mall
Suite 1500
Sacramento, CA 95814
Tel: +1 916 321 4800
Fax: +1 916 321 4900

www.kslaw.com

uniquely and durably authenticate an individual's identity when the individual accesses a physical location, device, system or account.

PII does not include information that is lawfully obtained from publicly available sources, including federal, state or local government records available to the general public.

Reportable Security Breach

A reportable "security breach" is the unauthorized acquisition of unencrypted computerized data, or of encrypted computerized data if acquired with the confidential process or key used to decrypt the data, that compromises the security, confidentiality or integrity of PII. "Compromise" is not explicitly defined by the statute. Like HIPAA, determining whether the data was compromised involves a risk analysis. However unlike the presumption of compromise built into HIPAA, the New Mexico law provides that breach notification is not required if after an investigation it is determined that the incident does not give rise to a significant risk of identity theft or fraud.

Breach Notification

A Person who "owns or licenses" PII must notify affected New Mexico residents of a "security breach" in the most expedient time possible, but not later than 45 calendar days following discovery. If 1,000 or more New Mexico residents are involved in a single security breach, the PII owner or licensor must notify, within the same time frame, the Office of the Attorney General and major consumer reporting agencies that compile and maintain files on consumers on a nationwide basis. Any Person who is licensed to maintain or possess computerized data containing PII must notify the owner(s) or licensor(s) PII of a "security breach" in the most expedient time possible, but not later than 45 calendar days following discovery. "Discovery" is not defined by statute; it is unclear whether the clock starts running at the time of actual knowledge or when a person "should have known." A 45-day notice period is longer than many states, and there are also two exceptions that provide even more time:

- When a law enforcement agency determines that the notification will impede a criminal investigation; or
- When delay is necessary to determine the scope of the security breach and restore the integrity, security and confidentiality of the data system.

Notification to affected residents must follow the methods described in the Act, unless the Person has breach notification procedures in place as part of information security policies that meet the timing requirements. In such cases, the Person's notification will be deemed compliant if it follows those policies and procedures in notifying residents of the breach.

The notice to affected residents must contain:

- The name and contact information of the notifying person;
- A description of the types of PII reasonably believed to have been the subject of a security breach (if known);
- The date/estimated date of the security breach, or the range of dates within which the security breach occurred, (if known);
- A general description of the incident;
- The toll-free telephone numbers and addresses of the major consumer reporting agencies; and
- Advice that recipients review personal account statements and credit reports, as applicable, to detect errors resulting from the security breach, and inform recipients of their rights pursuant to the federal Fair Credit Reporting Act.

Security Requirements

Unlike some states, New Mexico's breach notification law includes both information security requirements, aimed at preventing breaches, and breach notification requirements. Under the Act, those who own and license PII must:

1. Arrange for proper disposal of the records when they are no longer reasonably needed for business purposes. "Proper disposal" includes shredding, erasing or otherwise modifying the PII contained in the records to make it unreadable or undecipherable; and
2. Implement and maintain reasonable security procedures and practices appropriate to the nature of the PII to protect it from unauthorized access, destruction, use, modification or disclosure.

Contractor Agreements

Any Person subject to the Act who discloses PII pursuant to a contract with a "service provider" (anyone that receives, stores, maintains, licenses, processes or otherwise is permitted access to PII through providing services directly to a person that is "subject to regulation") must require by contract that the service provider implement and maintain reasonable security procedures and practices appropriate to the nature of the PII and to protect it from unauthorized access, destruction, use, modification or disclosure. Thus, health care companies that have avoided HIPAA business associate agreements will now be subject to similar contractual requirements under the Act. Further, like HIPAA, the contractual requirements will follow the flow of information from contractors to subcontractors because owners, licensors, and licensees of PII are "subject to regulation" under the Act.

Enforcement and Penalties

The New Mexico Attorney General may bring an action in the name of the state on the behalf of individuals alleging violations of the Act. In such an action, the court may:

- Issue an injunction; and
- Award damages for actual costs or losses, including consequential financial losses.

In addition, if the court determines that a person knowingly or recklessly violated the Act, it may impose a civil penalty of the greater of $25,000 or, in the case of failed notification, $10.00 per instance of failed notification up to a maximum of $150,000.

The Act does not provide a private right of action for violations. However, residents of other states where similar statutes provide no private right of action have found ways to sue.