June 1, 2018

Sweeping New Colorado Data Privacy Law Impacts Health Care Industry

On May 29, 2018, the governor of Colorado signed into law **HB 18-1128** (the "Privacy Law"), which made sweeping changes to Colorado's data privacy laws and which will affect nearly every Colorado business and government entity. The Privacy Law imposes new requirements on any person or entity that maintains, owns, or licenses personal information concerning Colorado residents, including health care entities that are "covered entities" for the purposes of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The Privacy Law's new requirements will take effect on **September 1, 2018**.

The Privacy Law imposes three main requirements, which are described in detail below: (1) a 30-day period in which to notify affected Colorado residents and the Colorado Attorney General of data security breaches; (2) a requirement to implement data disposal policies; and (3) a requirement to implement "reasonable security procedures and practices" to safeguard personally identifiable information. Although covered entities under HIPAA ("HIPAA Covered Entities") are to a large extent exempt from the new data disposal and security procedures requirements, HIPAA Covered Entities are not exempt from the new notification requirements.

New Requirements for Security Breach Notifications

The Privacy Law establishes detailed investigation and notification requirements for all "covered entities," defined as persons or entities that maintain, own, or license personal information in the course of their business, vocation, or occupation ("Colorado Covered Entities"). Comparable investigatory and notification requirements are imposed upon all governmental entities, including special districts such as hospital and health services districts. The Privacy Law also appears to have extraterritorial effect in that any business outside of Colorado that maintains, owns or licenses personal information concerning Colorado residents may be required to comply with the law or face consequences in Colorado courts.

The new investigation and notification requirements are tied to a security breach of personal information. The key terms are defined in the Privacy Law as follows:

- **"Personal information"** means a Colorado resident's first name or first initial and last name in combination with any one or more of the following data elements that relate to the resident when those data elements are not encrypted, redacted, or otherwise secured: **medical information; health insurance identification number; biometric data**; social security number; student, military, or passport identification number; or driver's license number or identification card. "Personal information" also includes a Colorado resident's username or email address, in combination with a password or security questions and answers that would permit access to an online account or a Colorado resident's account number, and a credit or debit card number in combination with an access code or password that would permit access to that account.
- **"Medical information"** means any information about a Colorado resident's medical or mental health treatment or diagnosis by a health care professional.
- **"Biometric data"** means unique biometric data generated from measurements or analysis of human body characteristics for the purpose of authenticating the individual when he or she accesses an online account.
- **"Security breach"** means the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information.

Once a Colorado Covered Entity becomes aware that a security breach may have occurred, the Colorado Covered Entity must:

- **First**, conduct in good faith a prompt investigation to determine the likelihood that personal information has been or will be misused;
- **Second**, unless the investigation determines that misuse of the personal information has not occurred and is not reasonably likely to occur, the Colorado Covered Entity must then give notice to Colorado residents affected by the breach. The notice must be made "in the most expedient time possible and without unreasonable delay, **but not later than thirty days after the date of determination that a security breach occurred**"—meaning the point in time at which there is a sufficient evidence to conclude that a security breach has taken place. The Privacy Law sets forth detailed requirements for information that the Colorado Covered Entity must include in the notices to affected residents. Additionally, the Privacy Law sets forth detailed requirements in the event that the personal information affected by the breach includes the Colorado resident's online account information or financial account information.
- **Third**, if more than 500 Colorado residents are affected by a breach, and unless the investigation determines that the misuse of information about a Colorado resident has not occurred and is not likely to occur, the Colorado Covered Entity must give notice to the Colorado Attorney General. The notice must be made "in the most expedient time possible and without unreasonable delay, **but not later than thirty days after the date of determination that a security breach occurred**."
- **Fourth**, if more than 1,000 Colorado residents are affected by a breach, the Colorado Covered Entity must also notify all consumer reporting agencies of the anticipated date of the notification to Colorado residents and the approximate number of people who are to be notified. The Colorado Covered Entity is not, however, required to provide the names or other personal information of the persons affected. The Privacy Law requires that notice be made to the reporting agencies in the "most expedient time possible and without unreasonable delay."

Finally, if a Colorado Covered Entity uses a third-party service provider—defined as an entity that has been contracted to maintain, store, or process personal information on behalf of a covered entity—that third-party service provider is required to give notice to and cooperate with the Colorado Covered Entity in the event of a security breach that compromises any computerized data containing personal information that the third-party service provider maintains on behalf of the Colorado Covered Entity. The third-party service provider is required to notify the Colorado Covered Entity "in the most expedient time possible, and without unreasonable delay, following discovery of a security breach, if misuse of personal information about a Colorado resident occurred or is likely to occur."

New Requirements for Data Disposal and Security Policies

The Privacy Law additionally requires Colorado Covered Entities to implement and maintain written policies for disposal of paper and electronic documents containing personal identifying information. The Privacy Law also requires that Colorado Covered Entities implement reasonable and appropriate security procedures and practices with regard to personal identifying information. With respect to third-party service providers to which the Colorado Covered Entity discloses personal identifying information, the Privacy Law requires the Colorado Covered Entity to require the third-party service provider to implement and maintain reasonable security procedures and practices, which are described in the Privacy Law.

These data disposal and security policy provisions apply to a more limited set of data than do the breach notification provisions. Specifically, these provisions apply to "personal identifying information," which is defined in the statute to mean a social security number; a personal identification number; a password; a pass code; an official state or government-issued driver's license or identification card number; a government passport number; biometric data; an employer, student, or military identification number; or a financial transaction device. That is, unlike the security breach requirements described above, the data disposal and security procdure requirements in the Privacy Law do not apply to medical information or to a health insurance identification number.

Additionally, a Colorado Covered Entity that is regulated by state or federal law and maintains procedures for disposal of information, as well as security procedures, is deemed to be in compliance with these Privacy Law provisions. Thus, Colorado Covered Entities that are already covered by, and in compliance with HIPAA, should be deemed to be in compliance with these new requirements, at least with regard to protected health information ("PHI") protected by HIPAA. HIPAA Covered Entities should determine whether they maintain, own, or license other types of data, apart from PHI, which may now need to be protected under the new Privacy Law.

Enforcement

The Colorado Attorney General may bring an action to address violations of the Privacy Law's new breach reporting, data disposal, and security requirements and may enforce compliance, recover damages resulting from a violation, or both. The Privacy Law also gives district attorneys the authority to prosecute criminal violations amounting to computer crime.

Although the new Privacy Law provisions are part of the Colorado Consumer Protection Act ("CCPA"), which provides a private cause of action in connection with certain "deceptive trade practices," it is unclear whether violations of the Privacy Law would give rise to a private cause of action under the CCPA. If a violation of the Privacy Law is interpreted to be a deceptive trade practice subject to the CCPA, a successful plaintiff could potentially recover treble damages and reasonable attorneys' fees from a Colorado Covered Entity.

Takeaways

Before the Privacy Law takes effect on September 1, 2018, HIPAA Covered Entities should:

- Review and revise breach response procedures to ensure that they will be able to promptly investigate and assess a potential security breach and comply with the new 30-day reporting time frame;
- Review business associate agreements to ensure that business associates are required to report breaches to the HIPAA Covered Entity in sufficient time for the entity to comply with the 30-day reporting time frame;
- Review, and if necessary, revise security policies and procedures affecting data protected by the Privacy Law;
- Determine whether they maintain, own, or license types of data that are not already regulated by state or federal law that may come under the new data disposal and security policy requirements;
- If the HIPAA Covered Entity does maintain, own, or license types of data that are not already regulated by state or federal law, determine whether it has disclosed such data to a third-party service provider and whether the entity must require that third-party service provider to implement and maintain the security procedures required by the Privacy Law.

If you would like help ensuring your organization is compliant with the new Privacy Law, please contact Brownstein for assistance.

Erin M. Eiselein
Shareholder
eeiselein@bhfs.com
303.223.1251

Sharon E. Caulfield
Shareholder
scaulfield@bhfs.com
303.223.1110

Anna-Liisa Mullis
Associate
amullis@bhfs.com
303.223.1165