Colorado Breach Notification Requirements: HB 18-1128

WHAT IS HOUSE BILL 18-1128?

Colorado Governor John Hickenlooper signed into law House Bill 18-1128 on May 29, 2018. The aim for this bill is to drastically improve privacy and security for all organizations within Colorado.

House Bill 18-1128 covers the following areas:

- Requires Covered Entities to protect personal information from unauthorized access, use, modification, disclosure, or destruction
- Requires Covered Entities to have written policies for the destruction and proper disposal of documents that maintain personal information
- Third party service organizations must implement and maintain reasonable security procedures to protect personal information
- Expanded requirements for breach notification for Covered Entities

Personal information includes a Colorado resident's:

- First name or first initial and last name in combination with one or more data elements that relate to the resident
- SSN
- Student, military, or passport identification number
- Driver's license or identification card number
- Medical information: Medical information includes any information about a consumer's medical or mental health treatment or diagnosis by a health care professional
- Health insurance identification number
- Biometric data
- Username or email in combination with password or security questions and answers
- Account number or credit or debit number with security codes

This bill overlaps and exceeds HIPAA requirements for Covered Entities; the notification requirements exceed HIPAA requirements.

NEW REQUIREMENTS FOR NOTIFICATION IN COLORADO

As the same with HIPAA, this bill requires that when a Covered Entity becomes aware a security breach may have occurred, the Covered Entity must in good faith prompt an investigation. When it has been discovered that a security breach has occurred, the Covered Entity must notify all those possibly affected by the breach.

HIPAA allows 60 days for this notification process, however House Bill 18-1128 allows 30 days for the notification process.

House Bill 18-1128 requires the notice to be:

- Written, to the postal address listed in the records of the Covered Entity;
- Telephone notice; or
- Electronic notice, if the primary means of communication by the Covered Entity with a Colorado resident is by electronic means.

Notice must be made in the most expedient time possible and without unreasonable delay, but no later than 30 days after the discovery date of the breach.

Third party service providers working with Covered Entity's who experience a breach, must give notice to and cooperate with the Covered Entity.

Source: House Bill 18-1128
http://leg.colorado.gov/sites/default/files/documents/2018A/bills/2018a_1128_signed.pdf

If a Covered Entity has a breach affecting more than one thousand Colorado residents of a security breach, the Covered Entity must also notify all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis of the anticipated date of notification to residents and the approximate number of residents who are to be notified. It is **not** required for the Covered Entity to provide the consumer reporting agency with the names or personal information of recipients.

If a Covered Entity has a breach affecting 500 or more residents, the Covered Entity must provide notice of the security breach to the Colorado Attorney General no later than 30 days after the discovery date if the breach.

The Attorney General may bring an action in law or equity to address violations of this law. The Attorney General has the authority to prosecute any criminal violations.

CONTENTS OF THE NOTICE

The contents of the notice must include:

- Date, estimated date or date range of the breach
- Description of the information acquired
- Methods to contact the Covered Entity
- Toll-free numbers, addresses, and websites for consumer reporting agencies
- Toll-free number, address, and website for the Federal Trade Commission
- Statement the resident can obtain information from the Federal Trade Commission and credit reporting agencies about Fraud alerts and security freezes
- If the affected individual(s) information breached included their electronic log in information, the affected individuals should be directed to promptly change his or her password and security questions and answers.

RESOURCES

It is recommended for Colorado Providers to review the law before it goes into effect on **September 1, 2018**. Click here to read House Bill 18-1128.

Source: House Bill 18-1128
http://leg.colorado.gov/sites/default/files/documents/2018A/bills/2018a_1128_signed.pdf