

Colorado Makes Sweeping Changes to Protect Consumer Data Privacy

August 6, 2018

By: Hilary Wells and Holly White

On May 29, 2018, Colorado governor John Hickenlooper signed into law House Bill 18-1128, which significantly expands existing privacy and data breach notification laws. Under the newly enacted legislation, covered entities that maintain paper or electronic documents with personal identifying information are to implement and maintain reasonable security procedures and practices. These entities will be required to investigate suspected security breaches and, when a security breach occurs, numerous notification requirements are triggered. The act takes effect on September 1, 2018.

Who is impacted by this law?

House Bill 18-1128 applies to “**covered entities**,” meaning any individual, legal or commercial entity, that maintains, owns, or licenses **personal identifying information** in the course of a business, vocation or occupation. Covered entities are required to implement and maintain reasonable security measures and practices to protect against the unauthorized use and access to personally identifying information for individuals that reside in Colorado.

What constitutes “**personal identifying information**?” Examples of this type of information include 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, which includes credit cards, debit cards, or account numbers that can be used to obtain cash, goods, property or used to make financial payments.

How do regulated entities comply?

A **covered entity** is regulated by state or federal law and is in compliance with House Bill 18-1128 when maintaining procedures for the protection of personal identifying information based on laws or guidelines established by its state or federal regulator. However, regulated entities may be required to notify consumer reporting agencies and/or the Colorado Attorney General of a security breach, depending on the number of affected Colorado residents.

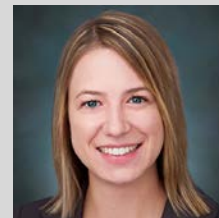
What is a non-regulated covered entity required to do?

For covered entities that are not subject to state or federal regulation, the new law establishes specific requirements:



Hilary Wells
Partner
303.628.9525 direct
hwells@lrrc.com
lrrc.com/wells

Hilary Wells is a partner in the firm’s Litigation practice group and serves as the chair for the firm’s Data Protection and Cybersecurity team. She has represented a wide-range of businesses including banks, financial advisors, private equity companies, insurance companies and health care providers. Hilary has tried cases in federal and state court as well as in arbitration.



Holly White
Associate
303.628.9572 direct
hwhite@lrrc.com
lrrc.com/white

Holly White’s practice focuses on large complex commercial litigation, insurance, cybersecurity, and health care law.

1. Develop a Written Policy

A non-regulated **covered entity** is required to develop a written policy for the destruction and proper disposal of paper and electronic documents containing **personal identifying information**. The written policy must require that, when such paper or electronic documents are no longer needed, the covered entity shall destroy the documents by shredding, erasing or otherwise modifying the personally identifiable information to make the information unreadable or indecipherable through any means. An exception to the destruction requirement applies if the covered entity is required by state or federal law to maintain the information for a longer period of time.

2. Implement and Maintain Reasonable Security Measures

A **covered entity** that maintains, owns or licenses **personal identifying information** of an individual residing in Colorado shall implement and maintain reasonable security procedures and practices that are appropriate to the nature of the personal identifying information and the nature and size of the business and its operations.

3. Investigate and Disclose Breaches

An obligation to investigate and disclose a breach is triggered when a **covered entity** becomes aware that a **security breach** that may have compromised **personal information** has occurred.

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 unencrypted data elements that relate to the resident: social security number; student, military, or passport identification number; driver's license number or identification card number; medical information; health insurance identification number; or biometric data;
- A Colorado resident's username or e-mail 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 or credit or debit card number in combination with any required security code, access code, or password that would permit access to that account.

A **covered entity** must give notice to the affected Colorado residents within **30 days** after it has determined that a **security breach** has occurred, unless the investigation determines that a misuse of information has not occurred and is not reasonably likely to occur. The new law specifies the categories of information that must be included in the notice. The covered entity may also be required to provide notice to consumer reporting agencies and/or the Colorado Attorney General, depending on the number of Colorado residents affected.

If you have any questions regarding House Bill 18-1128, including how to ensure your business is in compliance, please contact Hilary Wells (hwells@lrrc.com or 303-628-9529) or Holly White (hwhite@lrrc.com or 303-628-9572).

For information about HB 18-1128, please visit (<https://leg.colorado.gov/bills/hb18-1128>). Lewis Roca Rothgerber Christie maintains active commercial litigation and data security and privacy protection practices. For more information, please visit <http://www.lrrc.com>.