ISSUE BRIEF | House Bills 18-1211 & 18-1128

Colorado Attorney General's Priority Bills

Background

CHA closely monitored two bills advanced by the Colorado Office of the Attorney General that passed in the 2018 legislative session. One (HB 18-1211) codifies an existing unit in the Attorney General's Office first established through Executive Order, creating the Medicaid Fraud Control Unit, and the other (HB 18-1128) makes changes to the handling of consumer data privacy breaches in Colorado. Hospital and health system leaders should understand the requirements outlined in these two bills, as they will likely impact future hospital operations and processes.

HB 18-1211: Medicaid Fraud Control Unit

The bill codifies an existing unit in the Colorado Office of the Attorney General first established through an Executive Order in 1987, creating the Medicaid Fraud Control Unit (MFCU). The Attorney General's Office advanced this legislation to provide clarity to providers regarding what constitutes Medicaid fraud and waste under Colorado law, including that convictions for Medicaid fraud and waste are limited to providers who knowingly and willfully violate the law.

What You Need to Know

- The MFCU has the authority to investigate and prosecute fraud, misuse, waste and abuse committed by Medicaid providers as well as investigate and prosecute cases of patient abuse, neglect and exploitation.
- The Department of Health Care Policy and Financing (HCPF), the Colorado Department of Public Health and Environment (CDPHE) and managed care organizations are required to report suspected cases of fraud to the MFCU for investigation and pursuit of criminal and civil proceedings.
- HCPF may require that a notification be included in a patient's explanation of benefit that explains the process and contact information for reporting to MFCU suspected Medicaid fraud and waste or patient abuse, neglect and exploitation.
- "Intent to Defraud" is the standard used to prosecute Medicaid fraud and waste, which is consistent with the insurance code, Title 10.
- Absent knowing or willful conduct, a provider is not liable for Medicaid fraud and waste committed by a third party.

To ensure full compliance with this law, CHA recommends that all hospitals review the legislation's list of activities that constitute Medicaid fraud and waste as well as the penalties associated with each activity.

Continued

For questions or more information, contact Joshua Ewing, CHA manager, regulatory affairs, at 720.330.6061.

c|h|a Colorado Hospital Association

HB 18-1128: Protections for Consumer Data Privacy

This bill creates new state requirements for consumer data privacy, including imposing new procedures, timelines and state penalties for reporting breaches of "personally identifiable information," some of which are more strict than existing federal laws under the Health Insurance Portability and Accountability Act (HIPAA).

What You Need to Know

All HIPAA-covered entities, that are in full compliance with HIPPA, are also deemed compliant with the bill's record disposal and security procedure requirements. Hospitals must understand that under this new law, however, all HIPAA-covered entities must comply by Sept. 1, 2018, with new terminology, timelines for breach notifications and state-level penalties.

New Terminology:

- This bill uses the term "Personally Identifiable Information (PII)" instead of "Protected Health Information (PHI)" as used by HIPAA. PII includes 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.

New Breach Notification Requirements:

- Covered entities must give written notice to affected Colorado residents upon discovery of a security breach as soon as possible, but no later than **30 days** from the date of the breach.
- The breach notification to Colorado residents must include the date of the breach, a description of the information accessed in the breach and information for contacting credit agencies and the Federal Trade Commission.
- A covered entity is also required to provide notice to the Colorado Attorney General within **30 days** of any breach if the breach is believed to impact 500 or more Colorado residents. The Attorney General will investigate and prosecute the breach upon receipt of this notice.
- These new state-level notification requirements do not negate a HIPAA-covered entity's responsibility to also comply with HIPPA notification requirements.

New State-Level Penalties:

- If a patient's PII is compromised, HIPAA covered entities will be subject to federal financial penalties under HIPAA in addition to new state civil penalties and state civil damage under the Colorado Consumer Protection Act.

Additional Resources

- HB 18-1211 Final Bill and Fiscal Note
- HB 18-1211 will take effect on Jan. 1, 2019
- HB 18-1128 Final Bill and Fiscal Note
- HB 18-1128 will take effect on Sept. 1, 2018

For questions or more information, contact Joshua Ewing, CHA manager, regulatory affairs, at 720.330.6061.

c|h|a Colorado Hospital Association