POLSINELLI

July 2018

In This Issue

HIPAA-Covered Entities: It's Time to Cover Yourself

Are you prepared for Colorado's new data breach law to take effect?

By Iliana L. Peters and Colleen Guinn

On May 29, 2018, Colorado Governor John Hickenlooper signed changes to Colorado law that significantly increase potential data breach burdens and financial penalties on entities operating in Colorado.[1] Beginning September 1, 2018, any person – including a health care entity or professional – who maintains, owns, or licenses personal information must meet new requirements for storing and destroying information, as well as for alerting consumers of data breaches. Specifically, if an entity maintains the personal information of at least one Colorado resident, that entity must notify both the affected person(s) and the Colorado Attorney General of a breach "in the most expedient time possible," and no more than 30 days after discovery.[2] From a practical perspective, entities, including covered entities and business associates subject to the Health Insurance Portability and Accountability Act (HIPAA), should update existing policies, procedures, and forms to reflect the new data destruction and breach notification requirements, or risk facing significant penalties under the Colorado Consumer Protection Act. Healthcare entities especially should understand how the new law will affect them, and where it overlaps with and where it differs from existing requirements under HIPAA.

To Whom Does the New Law Apply?

HIPAA currently regulates the information practices of health plans, healthcare clearinghouses, and healthcare providers who transmit health information in electronic form using a HIPAA standard transaction. Many of the HIPAA regulations also extend to any "business associate" of one of these covered entities, defined as a person or entity that creates, receives, maintains or transmits regulated information or performs a service for, or on behalf of, a HIPAA covered entity, when the service involves access to regulated information.

Colorado's new law, HB 1128, defines the term "covered entity" for its purposes as "[a] person… that maintains, owns, or licenses personal identifying information in the course of the person's business, vocation, or occupation."[3] The law also extends to any "third-party service provider," meaning an entity "that has been contracted to maintain, store, or process personal identifying information on behalf of a covered entity."[4]

There are no general carve-outs in the Colorado law for entities already covered by HIPAA; so if your entity does any business in Colorado and is already subject to HIPAA regulations, it is important to be aware that HB 1128 imposes new, additional burdens.

---

[1] Ed Sealover, "Colorado governor signs law requiring more protection of consumer data," Denver Business Journal (May 29, 2018), https://www.bizjournals.com/denver/news/2018/05/29/colorado-governor-signs-law-requiring-more.html.

[2] 64152769.3

[3] HB 18-1128 at pg. 2.

[4] HB 18-1128 at pg. 6.

What Type of Information Must Entities Protect?

Under HIPAA, healthcare entities must protect the privacy and security of, and provide notification in the case of a breach of "protected health information (PHI)." This means entities must protect information that relates to an individual's past, present, or future physical or mental health condition, as well as to the provision of healthcare to an individual and the individual's payment. PHI includes not only diagnosis, billing, and other specific health information, but also names, addresses, dates of birth, Social Security numbers, and other identifying information.[5]

HB 1128 concerns the handling of two different categories of information. First, 1128 covered entities must implement reasonable security procedures and practices and employ proper disposal procedures for "personal identifying information." Personal identifying information includes Social Security numbers; personal identification numbers; passwords; pass codes; identification or driver's license numbers; employer, student, or military identification numbers; and financial transaction devices. Personal identifying information also includes biometric data, defined as "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."[6]

The law also covered entities that must abide by HB 1128's notification requirements when they experience a breach that affects "personal information." Personal information, in the context of a breach, has three possible definitions: 1) a Colorado resident's name in combination with at least one of the following: Social Security Number; student, military, or passport identification number; driver's license or ID number; medical information; health insurance identification number; or biometric data ("medical information" includes any information about an individual's medical or mental health treatment or diagnosis by a health care professional); 2) a Colorado resident's email and password; or 3) a Colorado resident's account or credit/debit card number in combination with a password or other method of accessing that account.

What Steps Should Entities Take to Protect Information?

HIPAA directs covered entities and business associates to implement "appropriate administrative, technical, and physical safeguards," which will "reasonably" limit disclosures of PHI.[7] HB 1128 similarly dictates that 1128 covered entities should "implement and maintain reasonable security procedures," as appropriate to the type of information and the size of the business[8]. Colorado law also mandates that covered entities destroy documents that contain personal identifying information once they are no longer needed, noting that the law provides that covered entities that have disposal procedures designed to comply with other state and federal laws are in compliance with the new requirement. As such, entities that do not otherwise have disposal procedures will need to undertake ongoing analysis of when information should be destroyed, keeping in mind that other state law requirements may apply, particularly with regard to the information of minors. As seen above, personal identifying information as defined under the Colorado law does not extend to medical information, but does cover a significant range of personal information.

What Must Entities Do in the Case of a Breach?

One area in which HIPAA and HB 1128 diverge is in their respective definitions of and requirements following a breach. HIPAA defines a breach as "the acquisition, access, use, or disclosure" of PHI.[9] Under HB 1128, a security breach is "the unauthorized acquisition of unencrypted computerized data that compromises the security, confidentiality, or integrity of personal information maintained by a covered entity."[10] Significantly, the mere access of protected information triggers HIPAA requirements – but in Colorado, access alone does not constitute a breach; personal information must be *acquired* to trigger the breach requirements.

So, what specific steps should entities take when a breach occurs? Under HIPAA, covered entities must, after they become aware of a breach, notify affected individuals, the U.S. Department of Health and Human Services, and potentially the media (if 500 or more individuals are affected). HIPAA dictates that notification should occur as soon as reasonable, and no longer than 60 days after discovery, although for breaches affecting fewer than 500 individuals, notification to HHS may be made within 60 days of the end of the calendar year in which the breach occurred. The notification itself must be a plain language description of what happened, the types of PHI involved, what the HIPAA covered entity or business associate is doing in response, what steps affected individuals should take, and relevant contact information. Notification should be written, sent by first-class mail, or by email if the individual agrees to electronic notice. Notably, HIPAA covered entities or business associates may undertake breach notification without assessing the risks to the PHI that may have been involved in the breach; risk assessment is only required under HIPAA if the entity wishes to determine that there is a low risk of compromise to the PHI involved, such that notification is not necessary. HIPAA covered entities and business associates should keep in mind that a breach only applies to unencrypted data – the law provides safe harbor for data that is encrypted to at least National Institute of Standards and Technology standards.

[5] Identifying information also includes geographic identifiers, relevant dates, telephone numbers, fax numbers, email addresses, social security numbers, medical record numbers, account numbers, license numbers, vehicle identifiers, device identifiers, URLs, IP addresses, biometric identifiers, full face photographic images, and other unique identifying numbers, characteristics, or codes. 45 C.F.R. § 164.514(b)(2).

[6] HB 18-1128 at pg. 4.

[7] 45 C.F.R. § 164.530(c).

[8] HB 18-1128 at pg. 3.

[9] 45 C.F.R. § 164.402.

[10] HB 1128 at pg. 6.

But entities cannot consider only HIPAA requirements in the case of a breach – they must also look to the burdens imposed by state law. In Colorado, requirements now noticeably differ from federal law. Under HB 1128, once an 1128 covered entity becomes aware of a security breach in which personal information was acquired, the entity *must* conduct a good faith investigation into the likelihood that the personal information has been or will be misused. Unless that investigation promptly determines that misuse of the information has not occurred and is unlikely to occur in the future, the entity only has 30 days after discovery of the breach to fulfill Colorado notification requirements. Similarly to HIPAA, a breach of encrypted information need only be disclosed if the encryption key was also acquired. The Colorado law imposes requirements on the entity to send notification to: 1) affected individuals in all cases, 2) to the state Attorney General in breaches affecting 500 or more individuals, and 3) for large-scale breaches affecting more than 1,000 individuals, the entity must also notify consumer reporting agencies. That notification should include: the date of the breach, a description of the information acquired, relevant contact information, and steps that individuals should take; however, entities that have individual notification procedures designed to comply with HIPAA can rely on those under the law, though they must still comply with the shorter time period. In contrast to HIPAA, 1128 covered entities have leeway in choosing whether this notice is in writing, by phone, or by email.

Entities should also note that under both HIPAA and Colorado law, notification requirements must be delayed (under HIPAA) or may be delayed (under Colorado law) pending criminal investigation, per the request of law enforcement.

What Penalties Do Entities Face for Non-Compliance?

Covered entities should be aware that both HIPAA and HB 1128 impose potentially costly penalties. HIPAA penalties increase in severity based on the level of culpability. For a HIPAA violation that the entity was unaware of and could not have realistically avoided, civil penalties of $112-$55,910 may be imposed for each violation, up to $1.68 million per year.[11] The minimum penalties increase significantly for violations that the entity should have been aware of but could not have avoided, were the result of willful neglect but were corrected, or were the result of willful neglect with no attempt to correct. HIPAA also provides for criminal penalties of up to 10 years in prison and $250,000 in fines.

HB 1128 was passed as an amendment to Colorado's Consumer Protection Act, and so the penalties previously set forth in that Act extend to violations of information protection requirements or notification requirements. The state law provides for civil penalties of up to $2,000 per violation, capped at $500,000 per related series of events. If victims are over 60 years of age, that number grows to potentially $10,000 per violation. The Colorado Consumer Protection Act also sets forth guidelines for civil actions. Entities could be liable for actual damages or $500, whichever is greater, plus attorneys' fees and costs. And if plaintiffs are able to provide clear and convincing evidence of bad faith, entities could potentially be held liable for up to three times actual damages (treble damages). The combination of civil penalties, criminal penalties, and civil damages under HIPAA and HB 1128 are potentially devastating for entities in non-compliance.

[11] Penalties are adjusted each year for inflation. The most recent numbers for 2017 can be found at 83 F.R. 9180 (Feb. 3, 2017).

How Do the Laws Affect Third Parties?

Many entities covered both by HIPAA and state data privacy laws rely on third-party relationships to carry out work or store information. As such, covered entities should also be aware of how the rules extend to those third parties. Under HIPAA, "business associates" include persons or entities that perform a service for, or on behalf of, a HIPAA covered entity, where the service involves the use or disclosure of PHI. Business associates also include subcontractors that create, receive, maintain, or transmit PHI.[12] The law requires that covered entities and their business associates have written agreements documenting their compliance. Those contracts have specific requirements, such as a description of the permitted uses of the PHI and the safeguards that the third party will use.[13]

HB 1128 also extends requirements to any third-party service provider, defined as "an entity that has been contracted to maintain, store, or process personal identifying information on behalf of a covered entity."[14] Entities covered by 1128 have a responsibility to require that their third-party service providers "implement and maintain reasonable security procedures and practices."[15] Those practices must be designed to protect personal identifying information "from unauthorized access, use, modification, disclosure, or destruction" (not just from a breach as it is defined under the law).[16] Further, third parties must notify the 1128 covered entity of any security breach "in the most expedient time possible."[17] In light of the new Colorado requirements, all HIPAA covered entities should take steps to revise their business associate agreements.

What Actions Should HIPAA Covered Entities and Business Associates in Colorado Take?

In light of the requirements discussed above, HIPAA covered entities and business associates should:

- Review, draft, and/or revise policies and procedures regarding the security of personal information to ensure that such policies and procedures provide for implementing reasonable security measures for that information, as necessary. To the extent that HIPAA covered entities and business associates have robust

[12] 45 C.F.R. 160.13(3)(iii).

[13] 45 C.F.R. 164.504(e) sets out the detailed requirements for these agreements.

[14] HB 18-1128 at pg. 4.

[15] Id.

[16] HB 18-1128 at pg. 3.

[17] HB 18-1128 at pg. 9.

policies and procedures designed to protect electronic PHI, as required by the HIPAA Security Rule, such policies and procedures will suffice.

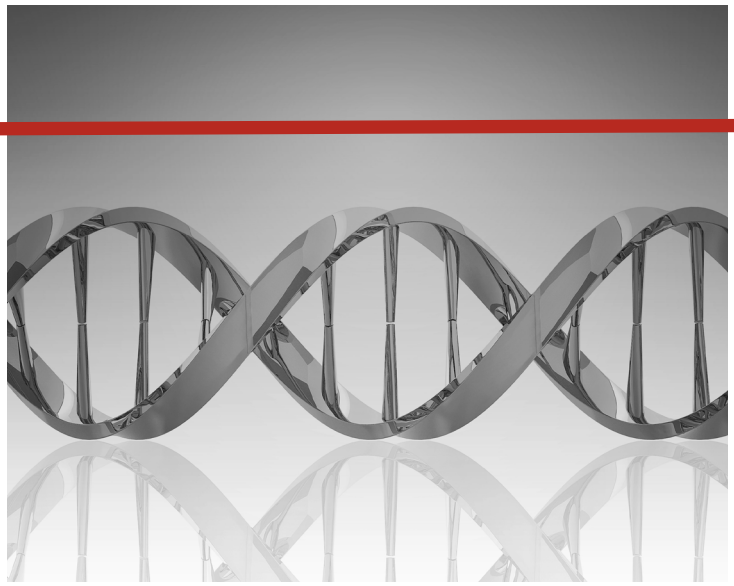
- Review, draft, and/or revise policies and procedures regarding the disposal of personal information to ensure that such policies and procedures provide for appropriate destruction of records, keeping in mind Colorado medical records retention requirement, as necessary.
- Review, draft, and/or revise breach notification policies and procedures to ensure that such policies and procedures provide for the investigation of breaches in which personal information was acquired to determine whether such information may be misused, and to ensure entities notify of such breaches within 30 days, including to the State Attorney General and consumer reporting agencies, as necessary; and
- Review, draft, and/or revise business associate policies and procedures and business associate agreements to ensure that business associates are required to report breaches to covered entities (or upstream business associates) as soon as reasonably possible, to ensure that such covered entities have sufficient time to undertake the required breach investigation under Colorado law, and to notify, as required, within 30 days;

Covered entities need to be aware of the state laws that affect them in regards to data breaches and notification requirements. And HIPAA covered entities should especially take note – come September 1st, entities will need to understand the unique new Colorado notification requirements that apply to them, and will almost certainly need to update their business associate agreements and any other relevant documents. If you have customers in Colorado, it is time to make sure that your business is covered.

Authors:

Iliana L. Peters
Shareholder
202.626.8327
ipeters@polsinelli.com

Colleen Guinn
Summer Associate
303.583.8275
cguinn@polsinelli.com



Learn more...

For questions regarding this information or to learn more about how it may impact your business, please contact one of the authors, a member of our **Health Care Services** practice, or your Polsinelli attorney.

To learn more about our **Health Care Services** practice, or to contact a member of our **Health Care Services** team, visit www.polsinelli.com/services/healthcare or visit our website at polsinelli.com.

About this Publication

Polsinelli provides this material for informational purposes only. The material provided herein is general and is not intended to be legal advice. Nothing herein should be relied upon or used without consulting a lawyer to consider your specific circumstances, possible changes to applicable laws, rules and regulations and other legal issues. Receipt of this material does not establish an attorney-client relationship.

Polsinelli is very proud of the results we obtain for our clients, but you should know that past results do not guarantee future results; that every case is different and must be judged on its own merits; and that the choice of a lawyer is an important decision and should not be based solely upon advertisements.

Polsinelli PC. Polsinelli LLP in California.