Jake Walker

Associate
303.293.5254
Denver
JSWalker@hollandhart.com

Beyond HIPAA: Navigating the "More Stringent" Standard

Insight — February 3, 2026

In light of the upcoming deadline for covered entities to update their Notice of Privacy Practices by February 16, 2026,[1] covered entities should consider “more stringent” state laws that may apply to these updated forms and require compliance. The Health Insurance Portability and Accountability Act (“HIPAA”) Privacy Rule (45 C.F.R. Part 164 Subpart E) sets the floor for privacy protections and rights of individuals when it comes to their individually identifiable health information, but allows for states to enact stronger or more stringent requirements regarding the privacy of patient health information. Where federal law sets the ground floor for compliance and allows states to set more demanding requirements as in the case with HIPAA, this is commonly known as “floor preemption.”[2] Thus, HIPAA leaves the door open for state law to impose standards more demanding than HIPAA in certain circumstances.

It is critical for covered entities to understand what state laws, if any, may impose additional obligations upon them, and that merely complying with HIPAA is not enough. This is made even more important by the raft of state-specific privacy protection laws that states across the country have implemented within the last decade. The examples below illustrate when and where state law may impose burdens more demanding than HIPAA and the Privacy Rule, but also note where HIPAA preempts other, conflicting state laws.

General Rule

Generally, state laws that (1) make it impossible for a covered entity or business associate to comply with both state and Federal requirements adopted under HIPAA, and (2) stand as an obstacle to accomplishing the purposes and objectives of the Administrative Simplification provisions of HIPAA, are preempted by HIPAA.[3] This general rule comes with certain exceptions, including the “more stringent” standard.

Specifically, if a provision of state law[4] that relates to the privacy of individually identifiable health information is “more stringent” than a requirement under the Privacy Rule, then the state law provision is not preempted by HIPAA.[5] When comparing a state law provision to a Privacy Rule requirement, a state law provision is generally considered “more stringent” where there are greater privacy protections for the individual.[6] For example, it may:

- set more restrictive limits on when Protected Health Information can be used or disclosed than HIPAA allows;
- expand an individual's rights to access or correct their PHI;

- demand more specific consent/authorization standards; or
- require more detailed accounting of disclosures or longer-lasting recordkeeping.

Notice of Privacy Practices

Within the Privacy Rule itself, the "more stringent" standard comes up in the context of Notice of Privacy Practices ("NPP") for PHI at 45 C.F.R. § 164.520. Specifically, when another applicable law is more stringent than HIPAA (e.g., 42 CFR Part 2 for substance use disorder ("SUD") records, or a more stringent state law), the NPP must adopt and reflect those more restrictive rules.

As mentioned above, given the upcoming NPP changes deadline to reflect changes for Part 2 records, covered entities need to analyze whether there are more stringent state laws to discuss as well.

Examples of "More Stringent" State Laws

The following are some examples state laws that potentially warrant further consideration for covered entities to include in NPP revisions.

- Colorado law prohibits providers or facilities licensed by the state from providing information (e.g., patient records) in furtherance of an out-of-state investigation (i.e., state or federal, to the extent constitutionally permissible) seeking to impose civil or criminal liability or professional sanction for engaging in certain "legally protected health-care activities" (e.g. seeking, providing, or receiving gender-affirming health-care services or reproductive health care that is lawful in Colorado).[7]
- New Mexico law prohibits health care providers and institutions from using or disclosing health information in an individual's electronic patient record to another person without the consent of the individual except as *required* by state or Federal law.[8]
- Montana law provides that when a patient requests to examine or copy all or part of their recorded health care information in writing, the health care provider must make such information available as promptly as required under the circumstances but not later than 10 days after receiving the request.[9]
- Nevada law requires a custodian of health care records to make a patient's records available for physical inspection by the patient, or the patient's representative designated in the patient's written authorization, within 10 working days if those records are located within the State of Nevada.[10] For records located outside the State of Nevada, the records must be made available to the patient or patient's designated representative within 20 working days of the request.[11] These response times are truncated further in the event of a request by a governmental investigator, grand jury, coroner, or medical examiner, to 5 working days or even less.[12]

Also, state laws governing health information and data privacy generally frequently exempt HIPAA covered entities, business associates, or PHI from applying under such laws.[13] The variety of state laws that may apply

to individuals' health information require close analysis, including not only their applicability, but also whether they impose a more stringent standard than HIPAA that applies in excess of HIPAA's threshold requirements. As covered entities prepare for the February 16, 2026, deadline to make appropriate updates to their NPPs, this analysis is even more important. Conducting it early, and correctly, can allow covered entities to ensure their Notice of Privacy Practices are up-to-date, accurate, and align with day-to-day practices with the most protective requirements, while avoiding complex and potentially costly questions of federal preemption and state control.

---

[1] *See* https://www.hollandhart.com/update-your-hipaa-notice-of-privacy-practices-by-february-16-2026.

[2] This also stands in contrast to “ceiling preemption,” where federal law sets the maximum standards and precludes any more restrictive (or differently restrictive) state laws from having effect.

[3] 45 C.F.R. § 160.203.

[4] “State law” is defined to include a constitution, statute, regulation, rule, common law, or other State action having the force and effect of law. *Id*. § 160.202 (defining “State law”).

[5] *Id.* § 160.203(b).

[6] *See id.* § 160.202 (defining “More stringent”).

[7] C.R.S. §§ 24-116-101 – 102.

[8] NMSA § 24-14B-6.A. As applied to Federal law, consent would be required in all cases except where required to be disclosed under HIPAA which occurs in two scenarios: when a patient requests access to their PHI or an accounting of disclosures of PHI; and, when HHS conducts a compliance investigation, undertakes enforcement action, or similar review. Previously the New Mexico law excepted as *allowed* by state or Federal law.

[9] MCA § 50-16-541.

[10] NRS § 629.061(1)(a), (2)(a); *see* NRS § 629.016 (defining “custodian of health care records” and “custodian”).

[11] *Id*. § 629.061(2)(b).

[12] *Id*. § 629.061(3).

[13] *See, e.g.*, NRS 603A.330(2)(b) (excluding covered entities and business associates from Nevada law requirements for providing notices regarding privacy of information collected via internet from consumers); *see also id*. § 603A.490(1)(a), (g) (excluding from applicability of state law governing security and privacy of consumer health data all entities subject to HIPAA,

including covered entities and business associates, and information used "only for public health activities and purposes" as defined in the Privacy Rule, whether or not such information is protected by HIPAA); *see also, e.g.*, C.R.S. § 6-1-1304(2) (The Colorado Privacy Act does not apply to protected health information that is collected, stored, and processed by a covered entity or its business associates, among other exclusions).
