Health Information Compliance Alert

Case Study: States Step Up As Federal HIPAA Enforcement Decreases

Tip: Review state rules before you outline your compliance plan.

HIPAA compliance remains a steady focus of the HHS Office for Civil Rights (OCR), but interestingly enough federal enforcement may be declining. However, as the feds target other systemic problems, states have tightened privacy and breach notification controls, creating stricter laws and bringing large-scale settlements.

Background: Under HIPAA, patients' individually identifiable health information is to be protected and kept private, according to regulations set forth in the HIPAA Privacy Rule. However, the Rule also makes allowances for state laws that are "more stringent" or "contrary" to the federal mandates, and this falls under its "preemption" guidance. What that means is that when a state's laws do not meet the federal standards or are "contrary" to the Rule, then HIPAA reigns. But, the opposite is true for states whose regulations go above and beyond or are "more stringent" than HIPAA.

"In the unusual case where a more stringent provision of state law is contrary to a provision of the Privacy Rule, the Privacy Rule provides an exception to preemption for the more stringent provision of state law, and the state law prevails," stresses OCR. The agency goes on to explain that "where the more stringent state law and Privacy Rule are not contrary, covered entities must comply with both laws."

Data security sits atop the list of most practices' to-do lists, particularly with social engineering, hacking, and malware attacks on the rise. Because of these issues, securing patients' protected health information (PHI) has never been more important. More so now than ever, it's vital that covered entities (CEs) review the gaps between federally-mandated HIPAA rules and state law updates.

Here's why: "The role of states has definitely increased in HIPAA enforcement," explains **Jim Sheldon-Dean**, founder and director of compliance services for **Lewis Creek Systems, LLC** in Charlotte, Vermont. "While there were more than a dozen enforcement resolution agreements handed down by HHS a couple of years ago, this year the rate seems to be about a quarter of that, so the pace of enforcement by HHS has certainly decreased."

Sheldon-Dean points out that the states have stepped in as the federal indictments have diminished. "State attorney generals are now picking up the slack, as they are permitted to do so under the HITECH Act enforcement provisions. Penalties in the hundreds of thousands of dollars have recently been levied in both Massachusetts and New York state in cases where the state AGs felt that HHS was not acting decisively enough, and so filed suit in federal court."

See How HIPAA Defines 'Contrary' and 'More Stringent'

It can be confusing to discern which path to follow - HIPAA or your state's law. With preemption wording, the best way to think of a "contrary" State law is to see it as an "obstacle" to following the HIPAA rules, according to section 160.202 of part 45 of the Code of Federal Regulations (CFR). A CE "would find it impossible to comply with both the state and federal requirements," and thus, would refer to HIPAA as the overarching mandate, OCR guidance notes.

However, for a state law to be considered "more stringent" and preempt HIPAA, they must outline protections that are more comprehensive than the criteria outlined in 45 CFR, section 160.202 and usually refer to specific areas of privacy and security coverage.

"These laws generally provide additional protection for sensitive categories of data, such as behavioral health information, HIV test results, genetic testing and counseling information and drug and alcohol treatment information," indicate attorneys **Dianne J. Bourque** and **Jordan T. Cohen** of national law firm **Mintz, Levin, Cohn, Ferris, Glovsky and Popeo, PC** in analysis of the Rules.

They write, "State laws impose additional compliance requirements. They may also overlap, conflict with, and in many cases, preempt HIPAA."

Review the nuances of 45 CFR, section 160.202 at www.gpo.gov/fdsys/pkg/CFR-2003-title45-vol1/xml/CFR-2003-title45-vol1-sec160-202.xml.

Prepare Now With Stronger Compliance Protocols

As regulatory reform continues to reshape the healthcare landscape, expect more changes to come down the pike as the states take on more of an enforcement role. In fact, over the last year many have clarified or updated their language on breach notification, encryption, personal information, timing, and more.

"Now all 50 states have some kind of a breach notification law, and states are adopting personal information privacy and security regulations, like the one California has slated for implementation in January of 2020," Sheldon-Dean says. "Already personal information protection is required of businesses in states like Massachusetts and Nevada, and [General Data Protection Regulation] GDPR-like privacy frameworks are in development at several levels of government."

Tip: If your practice assists patients across state lines, you are privy to HIPAA and every state regulation where you administer care. "Many of these state laws can be applicable across state lines, so healthcare entities need to consider the laws of the state of residence of all of their likely patients, not just their local state laws," reminds Sheldon-Dean.