Health Information Compliance Alert

Privacy: Review State Regulations to Ensure Compliance

Caution: State laws may be tougher than federal regulations.

Your organization may operate in a state that has more stringent privacy laws regarding health information than the HIPAA Privacy Rule. If that's the case, you'll need to reevaluate your policies to verify that you're following the stricter statute.

Why? Under HIPAA, covered entities (CEs) and their business associates (BAs) are charged with safeguarding patients' individually identifiable health information as part of the Privacy Rule. However, the provision also makes allowances for state laws that are "more stringent" or "contrary" to the federal mandates, and this falls under its "preemption" guidance. When a state's laws aren't as strict as the federal requirements or are contrary to the Rule, then HIPAA prevails. But, the opposite is true for states with regulations that 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 HHS Office for Civil Rights (OCR) guidance. "Where the more stringent state law and Privacy Rule are not contrary, covered entities must comply with both laws," the agency expounds.

"Luckily, a good job with HIPAA compliance can provide a good framework for compliance with all of the state laws an entity could be subject to," says **Jim Sheldon-Dean**, founder and director of compliance services for Lewis Creek Systems, LLC in Charlotte, Vermont.

Add These 7 Steps to Your State Compliance Planning

As part of your annual policy review process and risk assessment, you should crosscheck HIPAA against your state's privacy provisions. Consider these seven steps to help you ensure you're staying on target:

1. Review applicable state and local laws.
2. Look for differences between the various regulations and analyze your policies to ensure compliance with both.
3. Take extra precautions to check state regulations on hot privacy topics like identity theft, consumer rights, data misuse, texting, and online patient engagement.
4. Check state medical board policies on privacy, HIPAA, and state laws.
5. Ensure your EHR vendor is aware of any differences between state and federal requirements.
6. Implement practice policies that protect specialty-specific information that may extend beyond HIPAA.
7. Monitor regulatory reform at the state and federal level as privacy and security requirements evolve to meet the changing healthcare landscape.

Bottom line: Both privacy and cybersecurity breaches have increased during the pandemic - and state laws have continued to diverge from the federal regulations. That's why it's critical that your organization revisits its policies often and covers all the privacy bases to remain compliant. "Many of these rules call for the same precautions, safeguards, and procedures, and it's better to make your existing privacy documents more robust instead of creating parallel policies and procedures for each rule or law," advises Sheldon-Dean.