

Health Information Compliance Alert

Preemption Analysis MAKE A PREEMPTIVE STRIKE FOR COMPLIANCE

Sure, you're a pro with the privacy rule and you're well on your way to compliance, but if you're ignoring your state's privacy laws, don't pop open the champagne just yet.

There are literally hundreds of state and federal laws that govern access to personal health information. All states have laws that apply to protected health information. However, not all covered entities know what it takes to determine when the federal privacy rule preempts state laws.

What are the thresholds for preemption? What is really meant by the phrase "more stringent" as it relates to the privacy rule? Luckily, there are pages and pages of preemption guidance available for covered entities to digest.

One article, "Privacy Rule Demands Comparison of Federal and State Laws," authored by Cheri Jones for APA Online, reveals some of the basics you should be familiar with when planning a preemption analysis:

Know how your state's laws "relate to" PHI. Becoming familiar with your state law is the first step involved with a preemption analysis, according to Jones. Those laws include the state constitution, any statutes, regulations, rules, common laws or other state actions having the force or effect of law.

A privacy rule provision "relates to" PHI if its purpose is to protect the privacy of health information or if it affects the privacy of that information in a clear, direct and substantial way, according to Jones.

State vs. Federal Laws: Compare and Contrast

You'll have to compare the pertinent aspects of your state's privacy laws with the federal regulation to determine whether or not they're "contrary" to HIPAA's provisions, Jones urges.

"Contrary" means a covered entity finds it impossible to comply with both the federal and state law, and state law represents an obstacle to the accomplishment of the "full purposes and objectives" of HIPAA.

"Contrary" provisions can still stand, though, if they are exceptions to federal preemption as determined by the federal privacy rule, Jones notes.

Exceptions include the regulation of controlled substances, preventing fraud and abuse, regulating health plans and insurance, reporting on health care delivery or costs, and public health, safety or welfare.

Any person may request an exception, but the federal rule will remain in effect until the Department of Health and Human Services determines whether state law fits into an exception and if it will stay in effect.

Federal privacy laws don't preempt "more stringent" state provisions. A state law is more stringent when it contains greater patient privacy protections and permits greater access to patients to view or amend their health records. And according to Jones, state courts rule over disputes of the stringency of state law.

When in Doubt, Ask a Lawyer

While Jones offers some of the routine steps one can take to initiate a preemption analysis, others say it's probably best to seek outside counsel in such matters for a number of reasons.

"Frankly, my knee-jerk reaction is that the first step [privacy officers] should take [with preemption analyses] is to get a

lawyer," warns Tom Schroeder, a partner with the Minneapolis office of Faegre & Benson.

"It is such a minefield of judgments, and to make a misjudgment can blow up your privacy policies and leave you with no confidence or ability to judge your own compliance," Schroeder says.

But Schroeder says one need not shell out the big bucks for comprehensive guides to state law preemption. He anticipates that most small facilities might be better served — and feel less of a pinch — by acquiring some of the shorter legal memoranda that focus on the more significant aspects of state law most likely to continue to govern privacy preemption.

A crucial point to consider is that if you do seek legal counsel, you have protection under the "advice of counsel" defense, Schroeder adds. "If a client relies on advice of their legal counsel and that advice is incorrect, the client has a defense."

And, in fact, the HIPAA regulations incorporate a regulatory equivalent of that advice of counsel defense, and you basically get credit for that trust in your lawyer.

On the other hand, if you were to buy a compliance product from, say, your hospital association, then that's an entirely different situation. "You don't get advice of counsel defense and I doubt very much that [the Office for Civil Rights] is going to be very sympathetic to your pleas" if the preemption tool you purchased missed a step, says Schroeder.

"So I do think that for those key structural issues, advice of counsel is important and will also help tailor the advice to the particular facility's circumstances," adds Schroeder.

Schroeder says he's created a "thought chart" for his clients that consists of a step-by-step onepage decision tree. Clients answer questions in the order presented by the decision tree, which allows them to render conclusions based on the compliance needs of the facility.

The price for the chart varies depending on the circumstances of the client, Schroeder says, but the tool goes for less than \$1000, and he says similar charts created by other firms are widely available.

But Schroeder says that for anyone who has even thought about the preemption issue, they've already won half the battle.

He says the majority of the CEs are overlooking the impact of state law entirely. "They're even crafting policies entitled 'HIPAA compliance,' when for all they know, the majority of the compliance [consists of] state law privacy issues."