COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 20, Number 12. December 10, 2020 When AGs Call, Know When to Fight, When to Fold

By Theresa Defino

Transparency and contrition are two qualities that HIPAA officials at covered entities (CEs) and business associates (BAs) might want to think about expressing should they ever get a call from a state attorney general (AG) investigating a breach.

That's according to Jonathan Skrmetti, Tennessee's chief deputy AG, who spoke recently at the 2020 Healthcare Enforcement Compliance Conference, sponsored by the Health Care Compliance Association, which publishes *RPP*.[1]

Skrmetti addressed the growing interest that state AGs have in pursuing multistate settlements and the structure that supports these enforcement actions (see related story, p. 1).[2]

Of particular interest to compliance officials may be Skrmetti's insights into what AGs are looking for from CEs and BAs during the investigative and settlement process, what might win them points and what they shouldn't do.

'Fix What You Can'

By the time states start looking into a breach, the CE or BA should already have taken a number of actions, said Skrmetti.

"You want your case to be as uninteresting as possible" to authorities, he said. "You want to remediate upfront as much as you can. Obviously, you have to preserve some evidence, for forensic review. We're not saying the day you discover the breach you should be flying into a frenzy to get ahead of yourself and fix everything. But you need to be proactive about it, from our perspective, to make the case less interesting. Fix what you can, as soon as you can. Don't wait for the government to tell you what you need to do on that front."

He advised that for CEs and BAs that "want to move past the case quickly and get back onto the post-litigation world, transparency and contrition are your best route."

To begin, start talking early. "You really want to raise your arguments in the context of talking with the multistate negotiators at the outset of a settlement conversation," he said.

Skrmetti added that "litigating the merits with the states is a particularly rough path to go down because there are a lot of states, and so you're not just talking about a couple suits," but there may be "20, 30, 40 suits in state courts," and individuals from each state will need to be involved.

Develop Thoughtful Responses

He also offered the following additional recommendations.

Resist the urge to fight. "With litigators, the initial response is almost always to buck up and start fighting, but the settlement can be path-dependent to some extent. So, you really want to consider your posture from the get-

go and think about whether it's ultimately in [the CE or BA's] best interest to be contentious about it."

Consider how much to fight. Before moving forward, "the potential defenses are taken into account," by AGs, Skrmetti said. "Obviously it's your right to litigate, and there may well be instances where the government gets it wrong. But so far, we've done a pretty good job of identifying the breaches that need attention and giving them an appropriate amount of attention, at least from my perspective." State authorities who contact a CE or BA have already invested a lot of time, and "at that point, the states don't want to hear, 'We did nothing wrong. You guys are terrible. Here are all the reasons why you shouldn't be going ahead with this.'"

And what to fight about. "You can't be persuasive on certain issues," he said. "That's not to say there's no room for lawyering. For instance, [with] willful neglect, you may want to address the level of *mens rea* involved," said Skrmetti, referring to the organization's level of knowledge about the breach or its cause.

Narrow the focus. "We're lawyers; we expect legal arguments. But the way to do it is to keep your focus as narrow as possible, put out your strongest arguments, and explain to the states why they're just wrong with those particular points," he said. "The broader the arguments you raise, the more arguments you raise, the more likely any good ones you have are going to be lost in the overall litigiousness, and the states will be less inclined to reach a good settlement."

Beware the cost spiral. There will be a "common core of discovery" questions that "mitigate some of the redundancy there, but there are going to be a lot of state-specific discovery questions if things look like they are moving in a real litigation direction, and costs can really very quickly spiral to unreasonable heights if you start actually litigating in all the states," said Skrmetti.

Be truthful but don't 'oversell.' In responding to AGs, what state officials are "looking for is a clear, coherent and complete narrative that explains what went wrong, why it happened and why it's not going to happen again," Skrmetti said. He warned against exaggerations. "You don't want to say, 'We are the impenetrable fortress of data security and but for this one, tiny exploit, no patient data would ever be vulnerable.' Don't oversell it." Responses can include "a description of all the great security measures you had in place," which AGs understand "weren't enough" to stop the breach from happening, he said.

Be contrite. Show that, following a breach, "you feel terrible about it. You're going to fix it and make sure that going forward, things are much safer. That's going to put you in a much better posture as far as the state enforcers are concerned," said Skrmetti.

Don't send 'the wrong message.' Trying to minimize a breach "sends exactly the wrong message," he said. Organizations should not aggressively contest "every element of what the state's looking at or the states are looking at. If you're contesting jurisdiction in a frivolous way or a way that could be interpreted as frivolous, if you're litigating the merits without regard to the strength of your arguments in different areas, that's going to be putting you in a bad spot," Skrmetti said.

Show a history of compliance. "We want to see that you're taking security seriously," said Skrmetti. Demonstrate that "you've been following your policies, you've got good policies that are actually in practice, that you're doing the things that you need to do and the slipup was out of character, or was something that was on track to be remedied, or was something that you hadn't considered," he said.

Contact Skrmetti at jonathan.skrmetti@ag.tn.gov.

1 Jonathan Skrmetti, Brian Stimson, and Timothy Noonan, "Trends and Best Practices in Healthcare Privacy and Security Investigations," 2020 Healthcare Enforcement Compliance Conference, Health Care Compliance

Association, November 16, 2020, https://bit.ly/39IasaV.
2 Theresa Defino, "New Enforcement Threat: 'Coordinated' AGs Pursuing Settlements Following Big Breaches," *Report on Patient Privacy* 20, no. 12 (December 2020).