COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 20, Number 12. December 10, 2020 New Enforcement Threat: 'Coordinated' AGs Pursuing Settlements Following Big Breaches

By Theresa Defino

In late September, Anthem Inc. entered into a $39.5 million settlement for a 2014 data breach that affected nearly 79 million individuals.[1] About a week later, CHS/Community Health Systems Inc. agreed to pay $5 million for a breach that same year; 6.1 million records had been hacked.[2]

Premera Blue Cross, in July of last year, agreed to pay $10 million for its 2015 breach that exposed the protected health information (PHI) of more than 10.4 million people.[3] More than half of that amount—$5.4 million—went to Washington State alone, as its state Attorney General (AG) Bob Ferguson had spearheaded the investigation.

Because these payments all came amid costly settlements announced by the HHS Office for Civil Rights (with the same organizations), HIPAA privacy and security officials might have missed the fact that all four settlements were not with OCR but were negotiated by state AGs working together.

Just two years after the first multistate agreement related to a data breach—the $900,000 settlement with Medical Informatics Engineering[4] —the AG community is now motivated and experienced when it comes to pursuing such settlements, explained Jonathan Skrmetti, Tennessee's chief deputy attorney general. Covered entities (CEs) and business associates (BAs) that experience breaches affecting multiple states should expect attention from groups of AGs working together, according to Skrmetti, whose office led the CHS settlement.

"Most large-scale HIPAA breaches, because they involve patients in multiple states—often many states—are going to provoke multistate coordination" from the attorneys general, said Skrmetti, adding that the state AG "community is highly coordinated." Skrmetti made his remarks at the 2020 Healthcare Enforcement Compliance Conference, sponsored by the Health Care Compliance Association, which publishes *RPP*.[5]

CEs and BAs may be familiar with cases that AGs more typically handle individually within their own state, but Skrmetti said there is also "a lot of multistate activity." The Premera settlement brought together 30 state AGs; CHS involved 28; and Anthem, 43. The Medical Informatics Engineering settlement, brokered by Indiana, included 15 other states.

Also speaking at the conference with Skrmetti was Brian Stimson, a partner with McDermott Will & Emery LLP, who reviewed how the 2009 HITECH Act "amended the enforcement regime to authorize state attorneys general to bring civil actions in federal district court for both injunctive relief and damages on behalf of their citizens who may be harmed by data breaches." Until October, Stimson was HHS's principal deputy general counsel where he was, he said, "responsible for the HIPAA portfolio."

Investigations may be "concurrent" or "parallel" between state and federal officials, Stimson said, with "joint" investigations a rarity. He noted there can be "different staging, meaning sometimes state attorneys general can proceed more quickly than OCR or vice versa."

States Gained Experience From Other Settlements

Stimson said the "primary limitation" on state AGs is a provision in the act that "essentially gives OCR via the secretary first dibs on cases involving willful neglect."

As a result, state AGs "have to wait to pursue those kinds of cases under HIPAA until the OCR has exhausted its enforcement activities," Stimson said. Although this "statutory mechanism affects willful neglect cases as to HIPAA, as a practical matter, it doesn't really impact the manner in which state attorneys general" bring cases, said Stimson, because state AGs "can bring claims under a host of state laws, be [they] breach notification, privacy or consumer protection laws."

To pursue data-related settlements, AGs are capitalizing on their experiences working together on a number of investigations and enforcement actions, said Skrmetti, citing cases related to antipollution devices disabled by Volkswagen, mortgage settlements, tech companies and opioid litigation. Nowadays, "it's very common for states to go forward" with multistate investigations, including those related to data privacy, he said.

AGs work together formally through the National Association of Attorneys General, and "they all get together pretty regularly" and have personal relationships, as do attorneys specifically focused on consumer protection and data privacy, he said. "So, it's easy to get the machinery rolling when it's time to do a multistate" enforcement action, according to Skrmetti. He noted that "quite a few" such actions are "ongoing during any given time."

Executive Committee Supports Lead States

Such cases are handled via a "well-established framework," said Skrmetti, with one or two lead states that "chart the course and do most of the work" on a case, supported by "six to 10 states" whose representatives serve on an executive committee and handle "discrete portions of the case."

Coordination helps leverage limited resources, Skrmetti said. "Most offices have between 50 and 200 attorneys," while a few states have a greater number, and these are "responsible for a variety of activities, including defending the legality of state actions, either litigating against or for the federal government, and various big constitutional cases. Most of them have criminal appellate jurisdiction, and then all the full panoply of consumer protection and anti-trust enforcement," he said, adding, "there's a lot going on that stretches the resources of an office pretty thin."

Most AGs have "a small group" handling data privacy cases and may or may not have a dedicated division, he said, and cases may be centered in a consumer protection or "tech-oriented" section of an AG office that "handles anything having to do with a computer, whether it's offensive or defensive," Skrmetti said.

In terms of which states generally take the lead in data privacy cases, Skrmetti said there are "quite a few…that step up from time to time," and "there does tend to be a bit of bias toward the eastern part of the country for whatever reason in these cases."

Connecticut AG William Tong led the Anthem investigation, which culminated in the settlement that his office said was "with a 43-state coalition and California." Connecticut received $3.8 million of the $39.5 million; California received $8.69 million.[6]

In addition to Connecticut, other active states are Illinois, New York, Massachusetts, Texas, Indiana, North Carolina and Pennsylvania, Skrmetti said.

Common Statutes Facilitate Coordination

Skrmetti said his own state of Tennessee has taken the lead on several cases and noted that "figuring out which states are the lead states and which states are on the executive committee is a pretty important first step to resolving things."

He added that AGs are making a "time investment" when they take on such a case and said "figuring out who's going to be on the executive committee can take multiple meetings sometimes."

Care also goes into selecting which cases to pursue. "Lots of breaches happen, and there's a filtering process," said Skrmetti. "If you've got the attention of a multistate [action], that means you've already made it through several layers of the filter. And that means the states are pretty sure that they ought to be looking at you. It takes a fair bit of work to coordinate one of these, get everybody moving in the same direction."

According to Skrmetti, "a lot of what gets litigated and investigated in these cases relates back to the state consumer protection laws, and AGs have very broad jurisdiction under those laws, but it varies state by state. So, you might think that would complicate engaging in multistate activity, but typically, the core of activity that's being investigated is going to be common enough across the various statutes involved that the states can coordinate" their actions.

He added that the "only differentiation" between states occurs when they file a complaint or a settlement in their respective state courts.

'Aggressive' States May Drive Settlements

Skrmetti also shared what AGs are seeking in data litigation and settlements.

The focus of multistate actions is "remediation of the noncompliance," Skrmetti said, with AGs "looking to make sure that things get fixed and that there's deterrence going forward." State laws don't always allow for AGs "to do a robust job of obtaining restitution for affected consumers, so the money in these cases is typically for deterrence purposes and not compensation."

He said that, "in a very broad sense, the states and the federal government are looking for the same thing; we want what they want. We all want to know that PHI is going to be secure going forward. And we want other covered entities to learn from the examples so that we don't have to see the same things happen over and over."

That doesn't mean individual AGs don't have—or express—specific goals.

"Interesting dynamics" come into play when settlement or litigation terms are drafted, said Skrmetti, likening the process to "herding cats." States may have different desires; some "tend to want to go along and just get the cases done." Others are "very aggressive and want very specific and significant consequences," he said.

The strategy is to "get everybody on board and moving in the same direction," he said, and states that typically "want more, get all the states to ask for more." Consequently, the "strictest states tend to get their way."

A "hefty fine" or "significant injunctive relief" may be imposed "even if most of the states are not particularly invested" in either, because a small number of states can "steer" a settlement in this direction. This explains why multistate settlements are "much more aggressive than the federal [settlement] might be in certain circumstances," Skrmetti said.

AGs Views Now 'More Nuanced'

Generally speaking, when negotiating a settlement, AGs "try to find reasonable resolutions and streamlined processes to help people efficiently resolve the legal problems and put their focus where it needs to be, which is on fixing the security problems and taking care of their patients," Skrmetti said.

Because states have more recently become victims of hacks themselves, attitudes have shifted.

Previously, states had "more of a zero-tolerance attitude," said Skrmetti. "But I think states now are starting to understand that being the victim of a hacking is essentially inevitable, and it's as much a matter of luck as anything, and that there are steps that you can and should take, but those don't necessarily guarantee that you're going to be able to protect the data of your folks."

As a result, states have "a more nuanced view of breaches" and can "differentiate more between the degree of either misconduct or negligence that produced a breach," Skrmetti said.

When dealing with state AGs, "transparency and contrition are your best route," Skrmetti said. For more specific strategies, see related story.[7] Contact Skrmetti at jonathan.skrmetti@ag.tn.gov.

1 The Office of Connecticut Attorney General William Tong, "Connecticut Leads $39.5 Million Multistate Settlement Over 2014 Anthem Data Breach," news release, September 30, 2020, https://bit.ly/2VLQkMY.
2 Herbert H. Slatery III, "AG Slatery Reaches $5 Million Multistate Settlement with Community Health Systems," news release, October 8, 2020, https://bit.ly/3qBlQv4.
3 Washington State Office of Attorney General Bob Ferguson, "Attorney General Ferguson's investigation into Premera data breach results in Premera paying $10 million over failure to protect sensitive patient data," news release, July 11, 2019, https://bit.ly/39LdLht.
4 Theresa Defino, "Generic 'Tester' Accounts Allowed Records Hack Triggering $1M in OCR, State AG Payments," *Report on Patient Privacy* 19 no. 6 (June 2019), https://bit.ly/3gjfiwx.
5 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.
6 State of California Department of Justice, Office of the Attorney General Xavier Becerra, "Attorney Becerra Announces $8.69 Million Settlement Against Anthem, Inc., Over Failure to Protect Patients' Personal Data," news release, September 30, 2020, https://bit.ly/33NR0pB.
7 Theresa Defino, "When AGs Call, Know When to Fight, When to Fold," *Report on Patient Privacy* 20, no. 12 (December 2020).