COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 19, Number 2. February 28, 2019 MD Who Gave Drug Rep EMR Access Begins Probation, Expresses Remorse for Criminal Act

By Theresa Defino

Eduardo Montaña, M.D., had never encountered a representative from Aegerion Pharmaceuticals before a woman walked into the pediatric cardiologist's Atlanta-area practice one day in February 2013. After she met his office staff, Montaña gave approval for her to come and talk to him.

Over the next two months, Montaña and the rep, and another individual from Aegerion, would work together to identify nearly three hundred patients who might be candidates for Juxtapid, an orphan drug approved that previous December for a rare type of inherited high cholesterol—in adults. In a decision he now calls a "mistake" and an "extreme outlier," Montaña shared protected health information (PHI) with the woman, and even gave the woman access to his electronic medical records (EMR) system.

Thus began a chapter that led to Montaña being charged with a rare criminal, albeit misdemeanor, violation of HIPAA, for which he was sentenced to six months' probation last month. He pled guilty in February 2018. In his first public comments on the ordeal, Montaña, through his attorney, tells *RPP* that his is a "cautionary tale."

Montaña is "disappointed and upset that this ever happened and wants to make sure that no one else makes the same mistake," T.C. Spencer Pryor, a partner with Alston & Bird LLP, tells *RPP*. Pryor says Montaña didn't learn he was under investigation until three years after his dealings with Aegerion.

Aegerion itself was also accused of HIPAA violations, but prosecution on felony charges was deferred under a broad $35 million plea agreement in 2017 that also addressed False Claims Act allegations. The case against Aegerion stemmed from a whistleblower suit brought by three former employees of the company.

As part of Aegerion's settlement, announced a year before Montaña's guilty plea, "Aegerion admitted that it conspired to obtain patients' personally identifiable health information, without patient authorization, for commercial gain," the U.S. Attorney's Office for Massachusetts announced. The firm agreed to adopt "enhanced compliance provisions" related to HIPAA.

The government accused Aegerion of pushing the medication for patients who did not have the disease, known as HoFH , and the specific diagnosis for which Juxtapid was approved, failing to "give health care providers complete and accurate information" about the condition and its diagnosis, and violating the terms of a safety plan (Juxtapid carries a black-box warning). At the time of approval in 2012, Juxtapid was estimated to cost $300,000 annually, and Aegerion employees were under pressure to make sales.

Aegerion was engaged in a conspiracy, the "object" of which was for its "sales employees to obtain and use HIPAA-protected health information without patient authorization in efforts to identify patients not previously diagnosed with HoFH, yet perceived by Aegerion as potentially suitable for Juxtapid treatment, and thereby achieve increased sales of Juxtapid consistent with market expectations set by" one of the company's executives, the government alleged.

Montaña's guilty plea garnered a fair amount of media coverage, including an accompanying photo of him

entering the courthouse in Boston. Originally scheduled for June of last year, Montaña's sentencing did not occur until Jan. 14. The Department of Justice, at the time in the midst of a government shutdown, did not issue its customary news release upon sentencing.

In contrast to his plea, his sentencing produced almost no news stories. In fact, some accounts simply reported —without using Montaña's name—that a cardiac physician who earlier pled guilty to HIPAA violations in connection with Aegerion had received a sentence of six months' probation and a fine of $5,000.

He could have received a year in prison, but probation was supported by prosecutors due to Montaña's cooperation and other factors. Pryor presented more than a dozen character letters on Montaña's behalf, penned by his children, and his current and former wives, among others.

RPP contacted Pryor and Montaña after the sentencing. Neither agreed to an interview, but Pryor emailed responses to all of the questions *RPP* submitted.

Montaña is "grateful" he can serve his probation "at home in Georgia rather than in Massachusetts where the case was based," Pryor tells *RPP*. "He is eager to move on with his life, including continuing to care for his patients, and put this event behind him."

Montaña Granted Remote Access

In Pryor's telling, Montaña's sole interest is to "provide the best possible care for his patients, and that is what he did." Pryor says only one patient ever took Juxtapid, and that Montaña "stands by all clinical treatment decisions he made."

Still, Montaña "acknowledges that he made a mistake in disclosing patient information to the sales rep without permission from his patients to do so." Pryor says that Montaña did not obtain the HIPAA-required authorizations signed by patients (or parents or other legal representatives given his was a pediatric population).

Pryor contends that Montaña "had a general consent form, which he believed at the time was sufficient. He now recognizes that it was not and that he needed to do more in order to comply with HIPAA." Since then, says Pryor, Montaña "has worked with a third party specializing in HIPAA policies and procedures to ensure he has a fully compliant practice from this point forward."

According to a "statement of facts" that Montaña agreed to as part of his plea, he acknowledged providing a sales rep with "his personal EMR access password" so that the representative could "remotely access…the EMR system and review his patients' PHI." On the same day, the two also exchanged text messages so that Montaña could explain "how to navigate the EMR system." The goal was to whittle down a six-page list of 280 patients to those who were approximately 16 years old. At one point, the sales rep concluded an email to Montaña with: "By the way, I am sending this to you from my personal email because of the patient info," a sentence she punctuated with a smiley face.

There was more to Montaña's case than just illegal access to patient records. Montaña agreed that he had sought a "grant" of $236,000 from Aegerion, with the hope that "his burgeoning relationship with Aegerion would help" him receive the funding, which he planned to use "to provide better cardiac screening resources to children." Pryor notes that "Montaña did not obtain the grant he applied for, or any money or other remuneration from Aegerion, for that matter."

Pryor says Montaña also didn't have a policy when it came to drug reps—but he now does.

His practice is composed of a "close knit group, many of whom have been with him for many years," Pryor says.

"Drug reps do not visit often, given the specialty nature of Dr. Montaña's practice." Montaña believed that the drug rep would provide him with time-saving administrative assistance for a drug with enormous potential for his patients, and that had complicated application and program enrollment requirements," he says.

Guilt By Association?

Less than a year earlier, another physician met a fate similar to Montaña's. In Rita Luthra's case, however, the cost was far higher. She was forced to surrender her medical license after she was arrested in connection with an osteoporosis medication manufacturer that was also under investigation. In October, she was sentenced to a one-year probation, which she is appealing. (See story, p. 10, for a look at her case and other criminal HIPAA prosecutions throughout the years.)

As Montaña's situation shows, working too closely—and inappropriately—with pharmaceutical companies puts individuals and organizations at greater risk because they are currently such a big target of prosecutors, says Laura Angelini, a partner with Hinckley Allen LLP.

Based in Boston, Angelini and her colleagues were recently moved to write an article for the medical news website *Stat* on this topic after witnessing the increasing number of HIPAA prosecutions in their own backyard. In fact, both Montaña and Luthra's cases originated in Massachusetts.

"The U.S. Attorney's office [in Massachusetts] has been very aggressive in terms of their health care fraud prosecution," she says. Activity may also be spurred by the number of pharmaceutical, life sciences and medical firms based there.

"Scrutiny" of drug manufacturers, pharmaceutical companies and their sales forces is not uncommon, she says. But the spotlight is widening to encompass "doctors, nurses and health care professionals" because they are "interacting with a population of people whose job it is to sell a drug to make money."

In the government's view, "pharmaceutical companies are up to no good—that's sort of the starting premise—and they're essentially using the doctors, nurses and medical staff to further their illegal conduct," says Angelini. "This is not what I think; this is in the eyes of the government," apparent in the cases it brings.

A "far-reaching" health care fraud case may turn on cooperation by people who are pleading guilty, says Angelini, who represents individuals and firms subject to government investigations. A possible HIPAA violation may turn up as a secondary issue, which is "a much easier thing to charge, and to prove, than a kick-back scheme, or an off-label marketing scheme where the jury might not really see the problem," she says.

In such cases, juries might believe there's nothing wrong if a patient might be helped. By contrast, a HIPAA violation might appear more black and white. "I think these criminal HIPAA violations have provided some really helpful leverage for prosecutors in trying to bring conclusion to some broader investigations," says Angelini.

Play It Safe

As a result, "if you have a doctor that is playing ball with the pharmaceutical company, or working the salesforce, that is definitely a risk area" for enforcement, she says.

Does this mean just saying no to all reps? Not necessarily, says Angelini. "When you're dealing with a salesforce in that type of context, you just have to make sure that they're not given access to any personal information…it's just not permitted."

While there might be "certain efficiencies…for the medical staff to have a sales rep come in and kind of look

through their electronic medical records for them to help them identify certain patients," signed patient authorizations must be in place, she says. Similarly, care must be taken with accepting meals, speaking fees and other honoraria.

Angelini points out the "strategy of a lot of pharmaceutical companies [is for] their sales force to have a presence" and develop a relationship with the physician and staff.

"There has to be a hard line between the medical professionals and any outside company, particularly a company that is looking to get the doctor and the doctor's office to give prescriptions for drugs because they're doing it to make money," says Angelini. Such an arrangement, if it goes wrong, implicates higher penalties because the actions may result in personal gain, she points out.

If providers have questions about whether their practices with third parties are violating or potentially violating HIPAA, "they should absolutely consult counsel. And obviously if they receive a subpoena or request to speak to a federal agent or a prosecutor, they should consult outside counsel. I can't emphasize that enough," she adds.

One option if problems are uncovered is to self-report to the government, an action "we've recommended to clients over the years. We always have to weigh the pros and cons of that decision."

One crucial step is to "make an educated assessment that you actually have a problem in the first place," she says.

One advantage may be more leniency on the part of government prosecutors who appreciate "that you came forward with information, particularly if it's something that they didn't know about…and maybe never would have discovered on their own," according to Angelini.

Covered entities and business associates must be clear about creating and enforcing a culture of compliance that does not tolerate violations—or violators, says Angelini, warning that employees who suspect there are problems have incentives to become whistleblowers.

Should the government come calling, it will be important to demonstrate "that you have a solid compliance plan in place, that you train your personnel on what the HIPAA rules are" and that training is periodically updated.

"The overarching theme and principle when you're dealing with prosecutors or regulators" is to recognize that "these agencies are very concerned and interested in what the organization's compliance structure is," Angelini says. "Stuff is gonna go wrong; inevitably it always does," and how the organization responds may be more significant than what actually happened.

Contact Pryor at spence.pryor@alston.com and Angelini at langelini@hinckleyallen.com. ✧