Historic State AG HIPAA Filing: An Important Case to Understand

By Iliana L. Peters, JD, LLM, CISSP, and Pasha Sternberg, JD

ON MAY 30, 2019, Medical Informatics Engineering, Inc. and its subsidiaries (collectively referred to in this article as "MIE"), agreed to pay $900,000 to 16 states that had jointly filed suit for violating the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Also, in late May, MIE settled for $100,000 with the US Department of Health and Human Services' (HHS') Office for Civil Rights (OCR) and agreed to begin a two-year plan to correct potential HIPAA violations. MIE's settlement with the 16 states marked the first time a significant number of State AGs banded together to file suit against a company for violating HIPAA. Although the suit was settled, the case is worth a close look as this collective state effort could have short- and long-term effects on health information management.

MIE provides a web-based electronic health record system to healthcare providers. Because the providers are covered entities (CEs) under HIPAA, MIE is a business associate (BA) and therefore subject to applicable HIPAA requirements and enforcement not only by HHS, but also by the State AGs, with regard to the individual patients who reside in their states, pursuant to the HITECH Act's expanded enforcement of HIPAA.

On December 3, 2018 twelve State Attorneys General (State AGs) jointly filed suit against MIE. Within weeks, four more states joined the suit, bringing the total to 16. In their complaint, the State AGs claim that a data breach impacting 3.9 million individuals, which MIE reported in 2015, was the result of MIE's failure to comply with multiple HIPAA and state law requirements, that MIE's response to the breach was deficient, and that by allowing a breach to occur after previously stating that it secures patient data, MIE had acted in a deceitful manner.

This case is noteworthy not only because of important lessons learned but also as an indicator of future regulatory actions by State AGs potentially affecting HIPAA-covered entities and BAs.

Brief Summary of the Data Breach

MIE's breach was the result of basic security failings that made its systems susceptible to a fairly straightforward and common attack. According to the complaint, in May 2015, threat actors identified two publicly accessible user accounts that were used by MIE to test its system. These accounts had very simple and common usernames —"tester" and "testing"—and passwords that matched the username. These weak credentials offered very little protection and, after either guessing or programmatically cracking these account credentials, the threat actor was easily able to gain access to the accounts.

In addition to having weak credentials, at least one of the accounts was susceptible to a SQL injection attack, a well-known and unsophisticated type of infringement that's been perpetrated for at least a decade. This attack allowed the threat actor to repeatedly query the account and obtain credentials to two other accounts. These subsequent accounts had administrator privileges, which gave the threat actor access to the system and the ability to exfiltrate unencrypted data that MIE held in its databases.

MIE was not aware of the breach until the volume of data that the threat actors exfiltrated grew to a size large enough to trigger an alert after slowing down network traffic. After the alert, it took MIE three days to investigate

the issue, identify what the attacker had done, and stop the data from being stolen.

MIE failures were not limited to pure technical issues; they also existed at an administrative level. The breach investigation revealed that MIE was aware of these weaknesses and the risks they posed well before the breach but had not taken steps to remediate the issues. In the time leading up to the breach, MIE had conducted at least two penetration tests that flagged the issues—one that flagged the two accounts' credentials and another that had identified the SQL susceptibility. Both penetration tests not only flagged the issues but also identified them as high risks.

Legal Framework and MIE's Compliance Failures

In their complaint, the AGs allege that MIE failed to comply with a number of legal requirements. They point specifically to violations of HIPAA Privacy and Security Rules and state law requirements that require companies to maintain reasonable security measures, notify individuals of a breach in a timely manner, and accurately state the level of security that a company has for the data it maintains.

HIPAA Technical Security Requirements

Also, in the complaint the AGs claim that MIE's security protections do not meet the standards of multiple HIPAA Security Rule standards. In their Complaint, the AGs allege that MIE failed to comply with numerous HIPAA Security Rule violations, including:

- Failing to review and modify security measures needed to maintain a reasonable and appropriate level of protection over ePHI
- Maintaining insufficient security measures to reduce risks and vulnerabilities to a reasonable and appropriate level
- Failing to regularly review records of information system activity
- Lacking mechanisms that record and examine activity in information systems
- Failing to identify and track users' access as well as authenticating users and not managing their access
- Not adequately encrypting the data it stored

With the complaint, the State AGs highlight the absence of an active security monitoring and alert system. Per the complaint, not having these types of protections is significant because had they been in place they would have alerted MIE to the presence of suspicious remote connections long before the network slowdown. The lack of this system would, therefore, be a potential violation of the Security Rule because MIE failed to review and modify security measures needed to maintain a reasonable and appropriate level of protection over electronic protected health information, implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level, implement procedures to regularly review records of information system activity, and implement mechanisms that record and examine activity in information systems, all of which are required by the regulations.

The complaint also faults MIE's lack of controls around how users accessed the network, including not identifying and tracking users, not authenticating users, and not managing user's access, all of which is also required by the Security Rule. Finally, the AGs identified the lack of encryption of the data that was exfiltrated as a final violation of the Security Rule's technology requirements.

HIPAA Administrative Requirements

In addition to the technical safeguard issues, the AGs cited MIE with deficiencies in meeting required administrative safeguards. The complaint specifically makes note of MIE's flawed incident response process and

its non-finalized and incomplete incident response plan. The AGs deem this to be a violation of HIPAA's requirement to have such a process in place and allude to the fact that the state of the incident response plan is representative of the quality of MIE's other policies and procedures. Similarly, the fact that MIE conducted risk analyses but did not remediate the risks that those analyses revealed is yet another administrative violation. Finally, the AGs' position is that the lack of controls on the amount of information that was accessible using the compromised accounts is an indication that MIE does not adhere to the Privacy Rule's minimum necessary standard. Notably, the complaint does not allege that MIE impermissibly disclosed information or any other Privacy Rule violation.

State Data Protection and Data Breach Notification Requirements

Separately from the HIPAA violations, the State AGs also argued that MIE violated various state laws. At the time of the breach, eight of the states—Arkansas, Florida, Iowa, Kansas, Louisiana, Minnesota, Nebraska, and North Carolina—had breach notification laws that required notification either within specific timelines or without unreasonable delay. The time between MIE's discovery of the breach and the notification of impacted individuals ranged from 52 days to more than six months, a violation of numerous state statutes, according to the AGs.

Additionally, five of the states—Arkansas, Florida, Indiana, Kansas, and Wisconsin—have laws that require companies to implement reasonable procedures to protect personal information.

According to the AGs, the same failings that trigger the HIPAA violations also create a violation of these statutes; in the complaint, the AGs are treating the lack of protections required by HIPAA as being unreasonable under the state laws, an important point regarding future potential enforcement of state laws applicable to data breaches.

Finally, the twelve states that originally filed the suit had statutes prohibiting unfair or deceptive trade practices. The AGs included allegations that MIE violated these statutes in their complaint, pointing to the fact that MIE had previously made public statutes in which they claimed that it would comply with HIPAA and would protect patient information.

The AGs argue in the complaint that the MIE promoted its ability to comply with HIPAA when promoting its services so not following through on these promises is a deceptive act. This deception is separate and apart from the underlying security violations and the failure to notify people of the data breach in a timely manner.

Putting the Case into Perspective

As discussed, there are a number of important aspects of this case. First, this case is unusual because it marked the first time that numerous State AGs have acted together to enforce HIPAA. The change of strategy by state regulators could be because MIE mishandled information about patients in multiple states. It is also noteworthy that MIE is a BA rather than a CE. Although HIPAA enforcement actions were routinely brought against CEs in the previous decade, the HITECH Act in 2009, which expanded jurisdiction over BAs, has increased the scrutiny on BAs. This lawsuit could be an indication that state regulators are becoming increasingly focused on underlying service providers like health record management system providers that interact with CEs' patient information.

Second, it is worth noting that that the complaint focuses mostly on violations of basic HIPAA Security Rule requirements. The types of security failures—weak credentials, lack of encryption, no user access controls, and no security monitoring—can be solved by fairly standard controls. In fact, it may have been that in this action the State AGs were enforcing the proverbial low-hanging fruit.

This case does not necessarily demonstrate that AGs are now expecting a state-of-the-art security framework. Instead, it's an indication that meeting the basics is likely a way to keep HIPAA CEs out of State AGs' crosshairs—for now.

Third, other than the minimum necessary standard, the AGs did not discuss the Privacy Rule and curiously did not include any claims that MIE improperly disclosed PHI. The Privacy Rule requires that both CEs and BAs disclose PHI only as permitted by the Privacy Rule, and an impermissible disclosure is and of itself a HIPAA violation.

Furthermore, the fact that the state law violations were imposed separately from, and not overlapping, the HIPAA claims is important because by separating the claims, the AGs settled regarding separate fines under each law.

Note that the AGs' imposed state claims required different duties on the part of BAs when compared to HIPAA requirements. As both HIPAA and the various state laws have significant penalties, this duplication can quickly increase the financial costs for the MIE.

While the AGs' unique approach to this case is significant, it is unlikely that this type of action will become the norm. This particular action was the result of a large breach impacting many individuals in multiple states.

In situations without similar footprints, it is unlikely that multiple AGs would focus their attention on an entity, and even more unlikely that they would coordinate their efforts. Additionally, as mentioned above, given the nature of the alleged security failings, the AGs were likely confident that they could prevail or reach a worthwhile settlement for purposes of sending a message about good baseline security safeguards to other vendors.

Finally, coordination among states takes a significant amount of resources. Even with the $900,000 settlement for the State AGs (and the $100,000 settlement with HHS), the State AGs likely invested much more in this case. Taken altogether, the handling of this case has significance, but multistate lawsuits are unlikely to become the norm.

Disclaimer: Polsinelli, LLP provides this material for informational purposes only. The choice of a lawyer is an important decision and should not be based solely upon publications.

Iliana L. Peters (ipeters@polsinelli.com) is shareholder and Pasha Sternberg (psternberg@polsinelli.com) is an associate at Polsinelli, LLP.

Article citation:
AHIMA. "Historic State AG HIPAA Filing: An Important Case to Understand" *Journal of AHIMA* 90, no.8 (August 2019): 20-22.