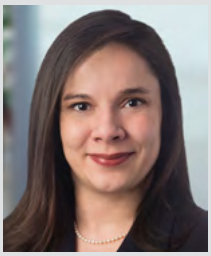
POLSINELLI®

Health Care Services

January 2019

Historic State AG HIPAA Filing: An Important Case We Are Watching

Authors:



Iliana L. Peters
Shareholder
202.626.8327
ipeters@polsinelli.com

Pavel (Pasha) A. Sternberg
Associate
415.248.2129
psternberg@polsinelli.com

In December 2018, twelve state Attorneys General ("AGs") jointly filed suit[1] against Medical Informatics Engineering, Inc. ("MIE") claiming it violated the Health Insurance Portability and Accountability Act and its related regulatory framework (collectively "HIPAA"), as well as various state laws.

Brief Summary of the Data Breach

In May 2015, a threat actor identified two publicly accessible accounts that MIE used to test its system. These accounts had very simple and common usernames and passwords that matched the username, which the threat actor either guessed or programmatically cracked. Once inside, the threat actor launched a SQL injection, a well-known and unsophisticated type of attack that's been perpetrated for at least a decade, to repeatedly query and obtain credentials for two other accounts. These subsequent accounts had administrator privileges, which gave them access to the system and the ability to exfiltrate unencrypted data.

Both of these weaknesses were known to MIE based on penetration tests they had done in the time leading up to the breach. To make matters worse, MIE only found out about the breach when the volume of data that the threat actor was exfiltrating got to be so large that it slowed down the network traffic and triggered an alert. Even 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.

Legal Framework and MIE's Compliance Failures

In their Complaint, the AGs allege that MIE failed to comply with a number HIPAA Security Rule violations, including:

- Failing to review and modify security measures needed to maintain a reasonable and appropriate level of protection over electronic protected health information (ePHI);
- Insufficient security measures to reduce risks and vulnerabilities to a reasonable and appropriate level;
- Irregularly reviewing records of information system activity;
- No 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; and
- Inadequately encrypting the data stored.[2]

---

[1] Complaint, *State of Indiana et al v. Medical Informatics Engineering, Inc.* et al, No. 3:18-cv-00969 (N.D. Ind. filed Dec. 3, 2018).

[2] 45 C.F.R. § 164.306(e); 45 C.F.R. § 164.308(a)(1)(ii)(B); 45 C.F.R. § 164.308(a)(1)(ii)(D); 45 C.F.R. § 164.312(b); 45 C.F.R. § 164.312(a)(2)(i); 45 C.F.R. § 312(c)(2)(d); 45 C.F.R. § 308(a)(4)(ii)(C); 45 C.F.R. § 164.312(a)(2)(iv).

Separately, the Complaint alleges various administrative failings such as no adequate Incident Response Plan, improperly conducting risk analyses and remediating issues based on those analyses and not adhering to the Privacy Rule's Minimum Necessary Standard.[3]

The AGs also argue that MIE violated various state data breach[4] and data protection[5] laws. Additionally, the AGs claim that MIE acted in violation of state unfair and deceptive trade practices statutes[6] by not living up to public claims that it would comply with HIPAA and would protect patient information.

State	Deceptive Acts	Data Breach	PIPA
Arizona:	Ariz. Rev. Stat. §§ 44-1528, 44-1534, and 44-1531		
Arkansas:	Ark. Code Ann. § 4-88- 113	Ark. Code Ann. § 4- 110-108	Ark. Code Ann. § 4-110-108
Florida:	Sections 501.207, 501.2075, and 501.2105, Florida Statutes	Section 501.171(9), Florida Statutes	Section 501.171(9), Florida Statutes
Indiana:	Ind. Code §§ 24-5-0.5- 4(C), and 24-5-0.5-4(G)		Ind. Code § 24-4.9-3-3.5(t)
Iowa:	Iowa Code § 714.16	Iowa Code § 715c.2	
Kansas:	Kan. Stat. §§ 50-632, and 50-636	Kan. Stat. § 50-7a02	Kan. Stat. § 50-6139b
Kentucky:	Ky. Rev. Stat. §§ 367.110-.300, and 367.990		
Louisiana:	La. Rev. Stat. § 51:1401 et seq.	La. Rev. Stat. 51:3071 et seq.	
Minnesota:	Minn. Stat. § 8.31	Minn. Stat. § 8.31	
Nebraska:	Neb. Rev. Stat. §§ 59- 1602; 59-1608, and 59- 1614	Neb. Rev. Stat. § 87¬806	
North Carolina:	N.C. Gen. Stat. § 75-1.1, et seq.	N.C. Gen. Stat. § 75-65	
Wisconsin:	Wis. Stat. §§ 93.20, 100.18, and 100.26		Wis. Stat. § 146.84(2)(b)

[3] 45 C.F.R. § 308(a)(6)(ii); 45 C.F.R. § 308(a)(1)(ii)(A); 45 C.F.R. § 164.502(b)(1).

[4] Ark. Code § 4-110-105; § 501.171, Fla. Stat.; Iowa Code § 715c.2; Kan. Stat. § 50-7a02; La. Rev. Stat. 51:3071; Minn. Stat. § 8.31; Neb. Rev. Stat. § 87-806; N.C. Gen. Stat. § 75-62.

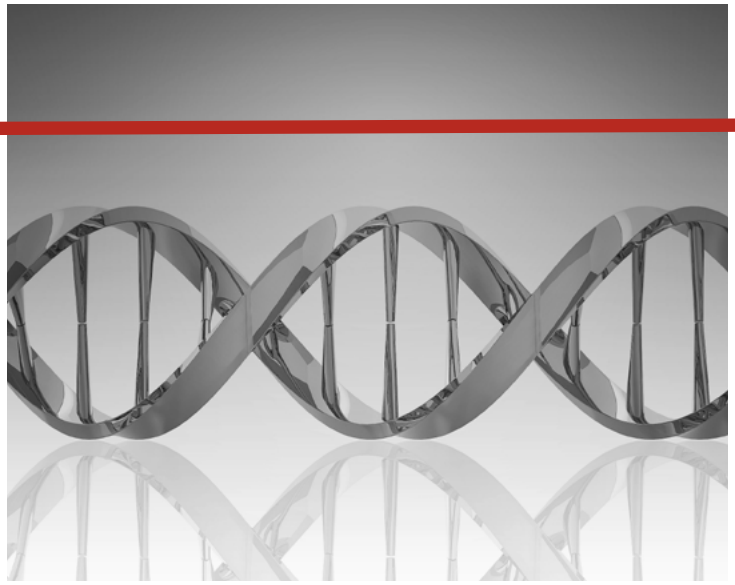
[5] Ark. Code Ann. § 4-110-108; § 501.171(9), Fla. Stat.; Ind. Code § 24-4.9-3-3.5; Kan. Stat. § 50-6, 139b; Wis. Stat. § 146.84(2)(b). Wisconsin words its statute slightly different than the other states; prohibiting "negligent disclosure" of information rather than requiring implementation of "reasonable" safeguards. Wis. Stat. § 146.84(2)(b).

[6] Ariz. Rev. Stat. § 44-1522; Ark. Code. § 4-88-101; § 501.204, Fla. Stat.; Ind. Code § 24-5-0.5-3; Iowa Code. § 714.16; Kan. Stat. § 50-626; Ky. Rev. Stat. § 367.170; La. Rev. Stat. § 51:1405; Minn. Stat. § 325F.69; Minn. Stat. § 325D.44; Neb. Rev. Stat. § 59-1602; N.C. Gen. Stat. § 75-1.1; Wis. Stat. § 100.20;

Putting the Case into Perspective

There are a number of noteworthy aspects of this case. First, it marks the first time that multiple State AGs have acted together to enforce HIPAA. Second, MIE is a Business Associate rather than a Covered Entity, and traditionally HIPAA enforcement actions have tended to be brought against Covered Entities rather than their Business Associates. Third, it is worth recognizing that the complaint focuses mostly on violations of basic HIPAA Security Rule requirements – MIE's security failures can be solved by standard controls, so the AGs are enforcing the proverbial low-hanging fruit. Fourth, 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. Finally, the fact that the state law violations were imposed separately from the HIPAA claims is very important because, by separating the claims, the AGs can impose separate fines under each law.

While these five elements make the case interesting and important, it is unlikely that this type of action will be taken often. This was a large breach impacting many individuals in multiple states and without such a fact pattern it is unlikely that multiple AGs would focus their joint attention on an entity, and even more unlikely that they would coordinate efforts. Additionally, the security failings here are very obvious so the AGs are likely confident that they can prevail or reach a worthwhile settlement. Finally, coordination amongst states takes a significant amount of resources. Taken altogether, this means that the health care field should certainly pay attention to this case, but likely does not mean that multi-state lawsuits will become the norm.



Learn more...

For questions regarding this information or to learn more about how it may impact your business, please contact one of the authors, a member of our **Health Care Services** practice, or your Polsinelli attorney.

To learn more about our **Health Care Services** practice, or to contact a member of our **Health Care Services** team, visit polsinelli.com/services/healthcare or visit our website at .

About this Publication

Polsinelli provides this material for informational purposes only. The material provided herein is general and is not intended to be legal advice. Nothing herein should be relied upon or used without consulting a lawyer to consider your specific circumstances, possible changes to applicable laws, rules and regulations and other legal issues. Receipt of this material does not establish an attorney-client relationship.

Polsinelli is very proud of the results we obtain for our clients, but you should know that past results do not guarantee future results; that every case is different and must be judged on its own merits; and that the choice of a lawyer is an important decision and should not be based solely upon advertisements.

Polsinelli PC. Polsinelli LLP in California.