Articles + Publications | October 30, 2020

28 States Resolve CHS Data Breach Investigation for $5M

WRITTEN BY

Christopher Carlson | Siran S. Faulders

Late last month, a coalition of 28 attorneys general announced a $5 million multistate settlement with Tennessee-based Community Health Systems, Inc. (CHS), stemming from the 2014 data breach that involved the personal information of 6.1 million Americans. Through the settlement, CHS also agreed to a series of data security and good governance provisions designed to strengthen its practices going forward. This resolution demonstrates (1) the continued focus on data privacy enforcement by state attorneys general and (2) the importance of developing a holistic data breach response plan that anticipates and can withstand scrutiny from state attorneys general and federal regulators.

Background

According to an independent investigation by the Office for Civil Rights at the U.S. Department of Health and Human Services (OCR), between April 2014 and June 2014, an unauthorized party accessed sensitive data held by CHS. In April 2014, the FBI notified CHS that it had traced a cyberhacking threat to CHS's information system. The hackers continued to access and exfiltrate the protected health information (PHI) of 6.1 million individuals until August 2014. Data breach notifications were then issued. According to OCR, the hackers used compromised administrative credentials to access CHS's information system remotely through its virtual private network.

Under the terms of the consent judgment with the state attorneys general, CHS agreed to a series of provisions designed to strengthen its security practices going forward. Detailed fully in the court order, CHS must:

- develop a written incident response plan;
- incorporate security awareness and privacy training for all personnel with access to PHI;
- limit unnecessary or inappropriate access to PHI; and
- implement specific policies and procedures regarding business associates, including use of business associate agreements and audits of business associates.

Less than a month before the settlement with the states, CHS reached a $2.3 million settlement with OCR related to the same security incident. This resolution required CHS to enter into a two-year corrective action plan to resolve alleged HIPAA violations arising from the data breach. OCR's press release declared that its investigation "found longstanding, systemic noncompliance with the HIPAA Security Rule including failure to conduct a risk analysis, and failures to implement information system activity review, security incident procedures, and access controls."

CHS also reached a $3.9 million class-action settlement in February 2019, offering up to $250 for related out-of-pocket expenses and up to $5,000 for those who experienced monetary losses due to identity theft or fraud resulting from the data breach.

Takeaways

Large scale data breaches will be scrutinized by state attorneys general

When it comes to investigating data security incidents, state attorneys general have become the top cop on the block. Many state attorney general offices, including those in Connecticut and Massachusetts, have formed dedicated consumer privacy and data security enforcement divisions. With this bolstered enforcement capacity, states previously limited in resources now have the manpower to lead nationwide investigations of data privacy incidents.

This is especially true for data breaches involving private health investigations. Since 2019, state attorneys general have taken actions in the following matters:

- For the first time, 16 states filed a federal data privacy action, alleging violations of the Health Insurance Portability and Accountability Act following a data breach. The matter filed against Medical Informatics Engineering was subsequently resolved for a $900,000 civil penalty and in conjunction with resolution of class claims and settlement with OCR.
- Thirty states, led by an all-West Coast leadership team of the California, Oregon, and Washington attorneys general, reached a $10 million multistate settlement with Premera Blue Cross concerning a data breach impacting 10.4 million patients.
- California reached a resolution with fertility-tracking app Glow, Inc. for alleged failures to adequately safeguard the personal, medical, or sensitive information of its users.

In the settlement with CHS, multiple attorneys general proclaimed the importance of protecting patient data:

- Tennessee Attorney General Herbert Slatery: “A patient’s personal information — especially health information — deserves the highest level of protection. This settlement will require CHS to provide that moving forward.”
- Ohio Attorney General Dave Yost: “Protecting patients is the job of a hospital and that includes shielding patients’ personal information from hackers.”

State attorneys general and the Office of Civil Rights offer a weighty one-two punch

When HIPAA is at play, the Office of Civil Rights has demonstrated a willingness to seek its own separate resolutions. These enforcement actions have not been limited to hospitals, but have been taken against health insurers, nonprofit health systems, orthopedic clinics, and solo practitioners.

This is the third data breach resolution this year, where the Office of Civil Rights has joined with state attorneys general to reach settlements. Mississippi Attorney General Lynn Fitch lauded the partnership, stating “I will continue to work with local, state, and federal partners to enforce laws that protect Mississippi consumers and stop bad actors who seek to compromise the integrity, security, and confidentiality of personal and private information.”

Combined state and federal enforcement actions have become commonplace. Thus, when a security incident involving patient data occurs, a company must be prepared to respond to both state and federal inquiries (in addition to the plethora of class actions that often hit simultaneously or shortly thereafter). Companies should also keep in mind that not all resolutions are the same. Instead, they can come in different forms — either through informal settlement agreements, agreements referred to as Assurances of Discontinuance or Assurance of Voluntary Compliance, or court-ordered consent judgments. The type of agreement depends on various factors that include whether there is a related federal settlement, the lead state that initiated the investigation, the participating group of states, and often the severity of the security incident. The nature of the agreement is often just as important as the terms, and companies should be mindful of this during the early stages of negotiation.

Conclusion

State attorneys general — and federal regulators — are continuing to bolster their data security enforcement capacities, and the CHS resolution that arose from a security incident that occurred more than a half decade ago demonstrates that companies must take all steps necessary to protect customer data. Moreover, it is imperative that companies have a security incident response plan in place, so if a data breach occurs, they have a road map to immediately identify what, if any, obligations they have to consumers, regulators, and law enforcement.

RELATED INDUSTRIES + PRACTICES

- Enforcement Actions + Investigations
- State Attorneys General