

New York Settles EmblemHealth Breach for \$575,000

Article By:

Kristi VanderLaan Kung

The recent \$575,000 [settlement](#) with EmblemHealth signals a push from AG Schneiderman “for stronger security laws and hold[ing] businesses accountable for protecting their customers’ personal data.” Noting New York’s “weak and outdated” security laws, AG Scheiderman used the settlement to urge for the swift passage of the Stop Hacks and Improve Electronic Data Security Act (“[SHIELD Act](#)”) introduced by his office in November 2017, which would make New York one of the most protective states in terms of data privacy and security.

In addition to the monetary fine, EmblemHealth agreed to implement a Corrective Action Plan and perform a comprehensive security risk assessment associated with the mailing of policy documents to policyholders. The risk assessment report must be submitted to the Attorney General’s office within 180 days of the settlement. EmblemHealth must also review and revise its policies and procedures based on the results of the risk assessment, and notify the Attorney General’s office of any action it takes.

Under the Corrective Action Plan, EmblemHealth must also conduct comprehensive workforce training relating to the incident and for a period of three (3) years, report security incidents involving the loss or compromise of New York residents’ information to the Attorney General’s office, even if they might not otherwise trigger the reporting requirements of New York State law.

The data breach, which involved the impermissible disclosure of Health Insurance Claim Numbers (which incorporated social security numbers), included members from multiple states in addition to New York. As a HIPAA-covered entity, EmblemHealth is also subject to enforcement by the Department of Health and Human Services Office for Civil Rights. This settlement underscores the fact that HIPAA does not preempt more restrictive state laws governing the privacy and security of protected health information and that states may independently take action against companies for breaches that impact their residents. The settlement addressed that the mailing error violated New York General Business Law § 399-ddd(2)(e) relating to the printing of an individual’s social security number on a postcard or other mailer not requiring an envelope, or visible on the envelope, or without the envelope having been opened.

Putting It Into Practice: Healthcare companies often (rightly) focus on HIPAA enforcement relating to the privacy and security of healthcare information; however, this settlement is a reminder that state laws are just as important and violations can subject companies to astronomical cumulative fines and costly compliance obligations. We will keep an eye on New

York's developments surrounding the SHIELD Act and what its passage may mean for companies doing business in New York or involving New York residents.

Copyright © 2025, Sheppard Mullin Richter & Hampton LLP.

National Law Review, Volume VIII, Number 74

Source URL: <https://natlawreview.com/article/new-york-settles-emblemhealth-breach-575000>