Codify
BY AAPC

Health Information Compliance Alert

Case Study: Follow 6 Steps To Avoid This Type Of Costly Data Breach

Data-breach class action lawsuit sets new practice in awarding damages.

"No harm, no foul" is no longer a valid catch-phrase for any HIPAA security breach case. And if a recent settlement agreement is an indication of how future breach cases will turn out, your risk exposure just got a lot more expensive.

Health insurer **AvMed**, **Inc**. recently entered into a settlement agreement through the **U.S. District Court for the Southern District of Florida,** in which the company has agreed to pay $3 million to resolve the allegations in a data-breach class action lawsuit.

Background: In December 2009, three unencrypted laptops were stolen from AvMed's corporate offices in Gainesville, FL, wrote Los Angeles-based attorney **Claire Readhead of Alston & Bird** LLP in a recent analysis of the case in the firm's privacy and security blog (www.alstonprivacy.com). And two of those laptops contained "sensitive information," including the protected health information (PHI) and Social Security numbers of 1.2 million AvMed members.

Members and other plaintiffs filed a class action lawsuit, claiming that AvMed failed to encrypt and safeguard the stolen laptop computers, which resulted in the exposure of the members' personal information, Readhead reported. AvMed filed a motion to dismiss, arguing that courts across the country have turned down data breach cases that failed to allege the lost or stolen data had been misused in a way that inflicts a compensable injury or damage to the plaintiff.

How the Settlement Payout Breaks Down

But the Florida court disagreed with AvMed's argument. According to a March 4 Health Law Rx Blog posting by healthcare attorney Elizabeth F. Hodge with Akerman LLP in Tampa, FL, AvMed settled the case and agreed to pay $3 million to a Settlement Fund, which will pay out:

- Up to $30 per AvMed member whose personal information was on the stolen laptops but who did not suffer identity theft. These members are part of the "Premium Overpayment Settlement Class," and the relief reimburses the members for the portion of premiums that they contended AvMed should have spent on adequate data protection.
- The reimbursable amount of any proven actual, monetary loss that occurred to each member as a result of the breach. This group of AvMed members is the "Identity Theft Settlement Class."
- $750,000 in attorneys' fees and costs for the plaintiffs' class.
- $10,000 as an incentive award, split evenly among the class representatives for their efforts in serving as class representatives.
- The costs of sending notices to the settlement classes, as well as all costs of settlement administration.

Why This Settlement Agreement Could Influence Future Cases

What sets this apart from other data breach settlements is that in this case, the "plaintiffs who have not suffered identity theft as a result of the breach may nevertheless collect from the Settlement Fund," Readhead explained. "Plaintiffs who did not suffer identity theft claimed they were injured by overpaying an insurance premium which was supposed to safeguard data."

What this means: "This settlement agreement demonstrates that healthcare providers, health plans, and their business associates may have increased exposure for damages in data breach lawsuits, even when plaintiffs cannot establish actual damages as a result of a breach," Hodge warned. "This settlement likely will serve as a model for future data security class action claims."

Beware that the AvMed settlement "marks a change in the traditional view of data breach damages," Readhead cautioned. So you should carefully review your insurance policies as well as your data security practices to mitigate your exposure.

Take These Actions to Protect Your Data Security

In addition to the hefty payout, AvMed agreed to implement the following actions, all of which Hodge asserted are excellent steps that you should also implement to minimize your risk of a costly data breach:

1. Provide mandatory security awareness and training programs for all employees;

2. **Provide mandatory training on appropriate laptop use and security** for all employees whose employment responsibilities include accessing information stored on company laptop computers;

3. Upgrade all laptop computers with additional security mechanisms, including GPS tracking technology;

4. Implement new password protocols and full disk encryption technology on all company desktops and laptops so that electronic data stored on those devices is encrypted at-rest;

5. Upgrade your physical security at company facilities and offices to further safeguard workstations from theft; and

6. Review and revise written policies and procedures to enhance information security.

Keep an Eye Out for 'Unjust Enrichment' Issue

Finally, another issue that came up in this lawsuit was the "unjust enrichment" theory. This is when plaintiffs claim that the insurer or provider should have used a portion of their health insurance premiums or medical care payments to improve data security.

"Plaintiffs have pleaded this unjust enrichment theory in other data breach cases in Florida courts without success," Hodge noted. "Time will tell if the AvMed settlement breathes new life into unjust enrichment and other novel data breach theories."

Link: To view the entire settlement agreement, go to www.akerman.com/documents/AvMed Data Breach Settlement Agreement.pdf.