Long-Term Care Survey Alert

Data Security: Your Risk Exposure Is Even More Expensive

Follow these 6 steps to ensure your facility doesn't take a hit.

The theft of three unencrypted laptops in 2009 resulted in a data-breach class action lawsuit against health insurer **AvMed, Inc.** in Florida. The whopping $3 million settlement carries a warning for all providers.

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.

Result: 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. The amount includes monies paid to each AvMed member whose personal information was on the stolen laptops but who did not suffer identify theft as well as the reimbursable amount of any proven actual, monetary loss that occurred to each member as a result of the breach.

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."

Bottom line: "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 facility 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 facility desktops and laptops so

that electronic data stored on those devices is encrypted at-rest;

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

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