CSR®
Data Life Cycle Management

Data Breach Cases Involving Fines and Other Penalties

Vermont Grocer Fined $15,000; Incurred Another $15,000 to Implement New System

Penalized for slow data breach response, Natural Provisions violated state's Security Breach Notice Act and Consumer Protection Act, failed to protect consumer data, and was required to implement new POS system

Natural Provisions stated the breach occurred because it "was unaware of legal obligations due to data breach…"

http://www.atg.state.vt.us/news/attorney-general-sorrell-requires-security-upgrades-and-assesses-penalty-for-security-breach-violations.php

Property Management Firm Fined $15,000

Stolen laptop with personal information (including social security numbers) of 600+ Massachusetts residents led to civil penalties.

The firm also must:

- Perform a compliance audit with its Written Information Security Program at least annually
- Effectively train employees on the policies and procedures with respect to maintaining the security of personal information
- Ensure personal information is not unnecessarily stored on portable devices
- Ensure all personal information stored on portable devices is properly encrypted
- Ensure that all portable devices containing personal information are stored in a secure

***Important Takeaway**:*

If your business owns, stores, or licenses the personal information of Massachusetts residents, as of March 1, 2010, you must have a written information security program – and that program must be appropriately vetted, implemented with proper training of employees, and it must be revisited from time to time to ensure that it is still consistent with your operations. Say what you do and make sure that you do what you say.

http://www.jdsupra.com/legalnews/massachusetts-attorney-general-data-brea-40449/

Small Business Data Breach Triggers $50,000 Fine

The Hospice of North Idaho agreed to pay the U.S. Department of Health and Human Services $50,000 to settle potential violations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule after a laptop was stolen containing sensitive information of 441 patients.

The hospice had not conducted a risk analysis to safeguard ePHI and did not have policies or procedures in place to address mobile device security as required by the HIPAA Security Rule.

http://www.hhs.gov/news/press/2013pres/01/20130102a.html