

## Report: More than 6M affected since breach notification rule

By *mmerrill*

Created 02/10/2011

CARPINTERIA, CA – Electronically protected health information (ePHI) has become a target for malicious attack, according to a recent report by Redspin, Inc., a provider of HIPAA risk analysis and IT security assessment services.

The report was conducted between August 2009 – when the HITECH breach notification interim final rule (IFR) went into effect - and the end of 2010. The findings were based on 225 security breaches affecting 6,067,751 individuals.

Redspin's analysis focuses on single breaches affecting more than 500 people. Such large scale breaches must be reported on a timely basis to individuals, the media and the HHS Secretary according to the HHS Office of Civil Rights' regulations. The regulations also require business associates of covered entities to notify the covered entity of such breaches at or by the business associate.

**[See also: [Missing files highlight need for tighter security](#)]**

Selected findings from the report include:

- 43 states, plus D.C. and Puerto Rico have suffered at least one breach affecting more than 500 individuals.
- 27,000 individuals, on average, are affected by a breach.
- 78 percent of all records breached are the result of 10 incidents, five of which are the result of theft of common storage media e.g. desktop computers, network servers, and portable devices.
- 61 percent of breaches are a result of malicious intent.
- 66,000 individuals, on average, are affected by a single breach of portable media.
- 40 percent of records breached involved business associates.

"Redspin is committed to helping covered entities and business associates properly safeguard private health information," said John Abraham, president and CEO of Redspin. "We hope that by highlighting these findings we can help healthcare organizations proactively address areas of highest risk."

**[See also: [Are you ready for a data breach?](#)]**

Redspin makes the following recommendations in its report for preventing breaches around four key areas:

- **Incident Detection and Response:** Implement an incident detection and response program to ensure all incidents are detected and responded to in a timely manner.
- **System Security Plan:** During the development of the next IT project develop a system security plan that documents each component of the new system, including external connections, where sensitive data is stored, who has access, what vulnerabilities exist with the system, and how to prevent those vulnerabilities from being exploited.
- **Portable Media Policy:** Rather than try to restrict where sensitive information is taken, take a data-driven view and focus on protecting data wherever it is stored. A mobile device security policy that includes management, operational and technical controls must be defined and implemented.
- **Business Associate Oversight:** Ensure your business associate oversight program includes a review of contractual language that requires business associates to take as much care with your protected health information as you do.

Read the full report [here](#).

**Source URL:** <http://www.healthcareitnews.com/news/report-more-6m-affected-breach-notification-rule>

**Links:**

[1] <http://www.healthcareitnews.com/../../../../news/missing-files-highlight-need-tighter-security>

[2] <http://www.healthcareitnews.com/../../../../blog/are-you-ready-data-breach>

[3] <http://www.redspin.com/resources/whitepapers-datasheets/>