Health Information Compliance Alert

Industry News: Data Security: Is It Really There In Healthcare Organizations?

No, if the latest HIMSS report is to be believed.

Are our PHI and other sensitive data as secure as we'd like them to be? No, if we go by the 2010 HIMSSAnalytics Report: Security of Patient Data. The biannual report clearly says healthcare organizations may be lulling themselves into a false sense of security when it comes to data security. And a post on www.hcfa.com says that this may have been the trend for too long now.

The report, which is a white paper commissioned by Nashville, Tenn.-based **Kroll Fraud Solutions,** says respondents gave their organizations high marks -- an average of 6 on a scale of 1 to 7 -- for compliance with HIPAA, state security laws, CMS regulations and the Federal Trade Commission's "Red Flags" rule for identity theft, and a score of 5.75 for compliance with new security requirements of the HITECH Act portion of the American Recovery and Reinvestment Act. But notwithstanding these high ratings, there were data-breach incidents in 19 percent of organizations in the past 12 months, up from 13 percent in 2008.

Human Error To Blame?

Of the total number of respondents, around 87 percent said they have policies to monitor access to and sharing of electronic health information, and that most of the reported breaches were due to sheer (avoidable) human carelessness -- stolen laptops and back-up tapes, as well as improper document disposal.

"On one hand, healthcare organizations are demonstrating increased awareness of the state of patient data security as a result of heightened regulatory activity and increased compliance," Kroll COO **Brian Lapidus** is quoted in the post as saying, "on the other, organizations are so afraid of being labeled 'noncompliant' that they overlook the bigger elephant in the room, the still-present risk and escalating costs associated with a data breach. We need to shift the industry focus from a 'check box' mentality around compliance to a more comprehensive, sustained look at data security."

Mobile Security: The Soft Underbelly

In yet another post on www.fiercemobilehealthcare.com, freelance journalist **Neil Versel** cites a 2008 survey by **Credant Technologies** that says a third of all healthcare professionals in America store patient data on portable and mobile devices such as USB drives, laptops and mobile phones, etc.

These mobile devices, according to Versel, are the soft underbelly of data security. Another report, Versel further says, found that 12,500 mobile devices were left in taxis, and 4,500 USB memory sticks were left in pockets of pants sent to dry cleaners during a six-month period in 2009. In spite of these scary statistics, only 39 percent of healthcare organizations encrypt data on mobile devices, a 2009 HIMSS survey revealed, Versel's post says.

Privacy and security experts are getting nervous about these grim statistics, and rightly so. Even the government has started acting tough which is reflected in the new, more-stringent HIPAA regulations either in place or on their way. For example, On Feb. 18, the maximum HHS civil penalty for a data breach jumped from $25,000 to $1.5 million.

"I'm always surprised at the cowboy attitude," **Harry Rhodes**, director of practice leadership for the American Health Information Management Association, said in an interview with American Medical News. "You've got these people who think, 'What are the odds of that happening to me?' And then when it's happening to you, it's too late to do anything."

(Editor's note: Read the post on hcfa.com at: www.hcfa.com/?p=24170. Versel's post can be read at:

www.fiercemobilehealthcare.com/story/healthcareorganizations-seemingly-lax-mobile-security/2010-02-23.The 2010 HIMSS Analytics Report can be downloaded from: www.krollfraudsolutions.com/about-kroll/HIMSSSecurity-Patient-Data.aspx.)