# ACA Raises Privacy, Security Concerns, Study Finds

Save to myBoK

*By Mary Butler*

While there was a slight decline in the number of healthcare data breaches in 2013, the risk of a breach event for a provider or one of their business associates is pervasive. This was one of the most notable findings in a recent Ponemon Institute webinar, “Affordable Care Act (ACA) Impacts on Patient Data Security.”

Ponemon Institute founder and chairman Dr. Larry Ponemon and ID Experts president and co-founder Rick Kam shared highlights from their “Fourth Annual Benchmark Study on Patient Privacy & Data Security” in an April 8 webinar. Both Ponemon and Kam admitted that they were surprised that their research detected a very slight downward trend in the number of reported patient data breaches. Ponemon investigators surveyed 505 healthcare organizations in 2013.

Kam said the finding surprised him “because the trend wasn’t pointing in that direction. It’s been increasing every year, and with business associates falling under [the HIPAA]-HITECH [Final Rule], I had presumed we’d see much more activity.”

According to the survey, 90 percent of healthcare organizations surveyed had at least one data breach in the last two years, with only 38 percent reporting more than five incidents. This marked a decline from the previous year’s report where 45 percent of organizations surveyed had more than five breaches. The economic impact of breaches also dropped 17 percent for participating organizations, from last year.

The improvement could be related to an increase in enforcement activities from the federal government and better access to risk assessment and self-auditing efforts by providers, Kam and Ponemon speculated.

## ACA Impacts on Privacy and Security

The Ponemon report also explored healthcare organizations’ perceptions of the Affordable Care Act’s impact on patient data security. The top three concerns among respondents, with regard to the new law, were:

- Insecure exchange of patient information between healthcare providers and the government
- Patient data on insecure databases
- Patient registration on insecure websites

This year’s survey, it should be noted, was completed prior to the close of the open enrollment period for health insurance through Healthcare.gov. The study period ended in January 2014, while the open enrollment period for the health insurance marketplaces closed March 31, 2014.

Provider concerns about ACA-related privacy and security issues stems from the constant media reports of user problems with the Healthcare.gov website, Ponemon and Kam said. When it comes to ACA initiatives such as accountable care organizations (ACOs), 51 percent of respondents said they were part of one, and 66 percent said risks for patient privacy and security due to the exchange of health information among participants has increased. However, when asked if participation in ACOs led to an increase in the number of unauthorized disclosures of personal health information (PHI), 41 percent said it was too early to tell, while 23 percent noted an increase.

Survey respondents were not very optimistic about security of health information exchanges (HIEs), either. Seventy-two percent of respondents said they were “somewhat confident” in the security of patient information exchanged in HIEs, and 40 percent said they were not confident about the security.

## Lingering Security Concerns

Ponemon noted that the very slight decrease in breach events doesn't mean organizations should rest on their laurels—rather, they should continue risk assessments and continue to take advantage of every tool they have to secure patient data. For example, while threats from inside an organization are still at the root of reported breaches, medical identity theft and criminal attacks on patient data are going up.

The study found that cases of criminal attacks on healthcare organizations have increased 100 percent since 2010. Ponemon said healthcare organizations used to consider medical identity theft as a consumer problem, but now they are starting to realize they play a role, too.

"These types of crimes can't be avoided completely, but increased awareness can lead to greater control. Definitely a large number of participants said a major concern was medical identity theft in their organization," Ponemon said in the webinar.

Another issue that's keeping privacy and security officials up at night, according to the report, is the proliferation of cloud-based file services. Only one-third of survey participants believe health data stored in cloud services is safe. Consumer-grade file sharing applications like Dropbox are also a concern.

"Now we're seeing broad use of these in healthcare and the data that's streaming into these tools are potentially high risk, confidential records," Ponemon said.

Kam added that criminals are starting to recognize the high financial value of protected health information, noting that "criminals are being more surgical about the kinds of information they're going after."

Click here for information on downloading the report and to listen to a recording of the webinar. Click here to download the report.

*Mary Butler (mary.butler@ahima.org) is the associate editor at the* Journal of AHIMA.

**Original source**:
Butler, Mary. "ACA Raises Privacy, Security Concerns, Study Finds" (Journal of AHIMA website), May 01, 2014.

Driving the Power of Knowledge