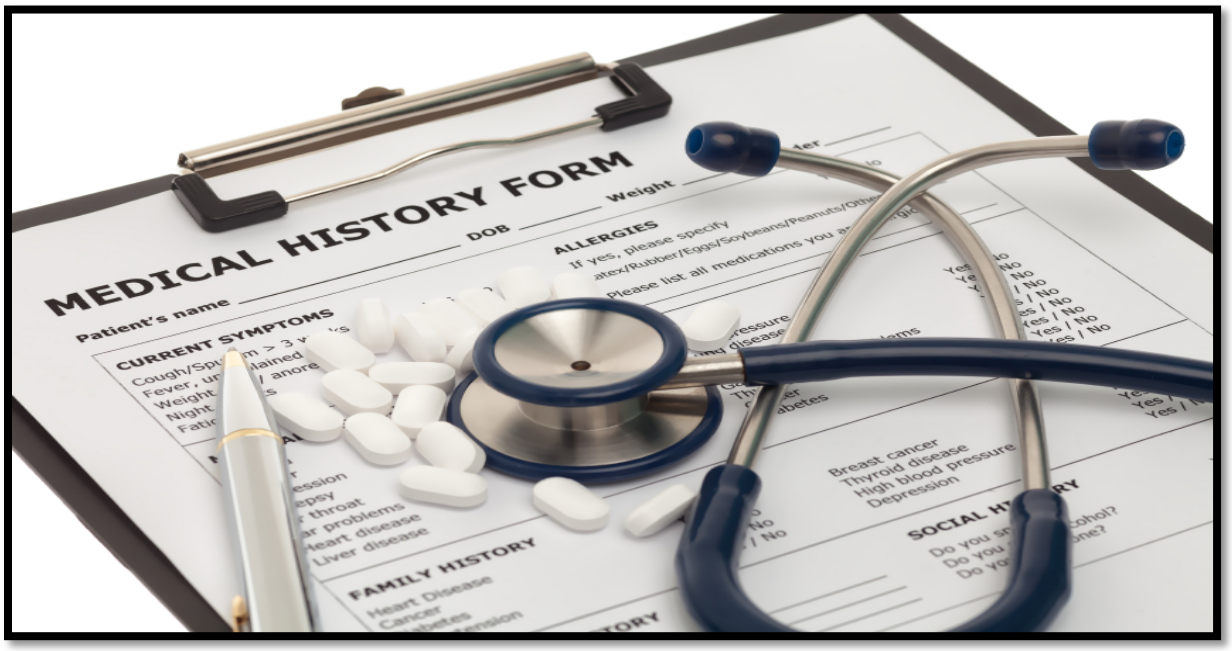
Ponemon INSTITUTE



Fourth Annual Benchmark Study on Patient Privacy & Data Security

Sponsored by ID Experts

Independently conducted by Ponemon Institute LLC

Publication Date: March 2014

Fourth Annual Benchmark Study on Patient Privacy & Data Security

Presented by Ponemon Institute
March 2014

Part 1. Introduction

The *Fourth Annual Study on Patient Privacy & Data Security* reveals new and expanded threats to the security and privacy of patient information in the U.S. healthcare system. The Affordable Care Act (ACA) is seen as a contributing factor because of the documented insecure websites, databases and health information exchanges that are highly vulnerable to insider and outsider threats. While the total number of data breaches has declined slightly over previous years, almost every healthcare organization represented in this research had a data breach. The study also found that healthcare organizations continue to struggle to comply with increasing complex federal and state privacy and security regulations.

Criminal attacks on healthcare systems have risen a startling 100 percent since we first conducted this study four years ago in 2010. Healthcare employees are fueling breach risks by increased use of their personal unsecured devices (smartphones, laptops and tablets). Business Associates—those that have access to PHI and work with healthcare organizations—are not yet in compliance with the HIPAA Final Rule.

Data breaches continue to cost some healthcare organizations millions of dollars every year. While the cost can range from less than $10,000 to more than $1 million, we calculate that the average cost for the organizations represented in this year's benchmark study is approximately $2 million over a two-year period. This is down from $2.4 million in last year's report as well as from the $2.2 million reported in 2011 and $2.1 million in 2010. Based on the experience of the healthcare organizations in this benchmark study, we believe the potential cost to the healthcare industry could be as much as $5.6 billion annually.[1]

The types of healthcare organizations participating in the study are hospitals or clinics that are part of a healthcare network (49 percent), integrated delivery systems (34 percent) and standalone hospital or clinic (17 percent). This year 91 healthcare organizations participated in this benchmark research and 388 interviews were conducted[2]. All organizations in this research are subject to HIPAA as a covered entity. Most respondents interviewed work in compliance, IT, patient services and privacy.

Key Research Findings:

The number of data breaches decrease slightly. Ninety percent of healthcare organizations in this study have had at least one data breach in the past two years. However, 38 percent report that they have had more than five incidents. This is a decline from last year's report when 45 percent of organizations had more than 5. This coupled with an increase in organizations' level of confidence in data breach detections suggests that modest improvements have been made in reducing threats to patient data.

Healthcare organizations improve ability to control data breach costs. The economic impact of one or more data breaches for healthcare organizations in this study ranges from less than $10,000 to more than $1 million over a two-year period. Based on the ranges reported by respondents, we calculated that the average economic impact of data breaches over the past two years for the healthcare organizations represented in this study is $2.0 million. This is a decrease of almost $400,000 or 17 percent since last year.

[1] This is based on multiplying $986,948 (50% of the average two year cost of a data breach experienced by the 91 healthcare organizations in this research) x 5,723 (the total number of registered US hospitals per the AHA).
[2] Benchmark research differs from survey research. The unit of analysis in benchmark research is the organization and in survey research it is the individual.

ACA increases risk to patient privacy and information security. Respondents in 69 percent of organizations represented believe the ACA significantly increases (36 percent) or increases (33 percent) risk to patient privacy and security. The primary concerns are insecure exchange of patient information between healthcare providers and government (75 percent of organizations), patient data on insecure databases (65 percent) and patient registration on insecure websites (63 percent of organizations).

ACO participation increases data breach risks. Fifty-one percent of organizations say they are part of an Accountable Care Organization (ACO) and 66 percent say the risks to patient privacy and security due to the exchange of patient health information among participants has increased. When asked if their organization experienced changes in the number of unauthorized disclosure of PHI, 41 percent say it is too early to tell. Twenty-three percent say they noticed an increase.

Confidence in the security of Health Information Exchanges (HIEs) remains low. An HIE is defined as the mobilization of healthcare information electronically across organizations within a region, community or hospital system. The percentage of organizations joining HIEs increased only slightly. This year, 32 percent say they are members and this is up slightly from 28 percent last year. One-third of organizations say they do not plan to become a member. The primary reason could be that 72 percent of respondents say they are only somewhat confident (32 percent) or not confident (40 percent) in the security and privacy of patient data share on HIEs.

Criminal attacks on healthcare organizations increase 100 percent since 2010. Insider negligence continues to be at the root of most data breaches reported in this study but a major challenge for healthcare organizations is addressing the criminal threat. These types of attacks on sensitive data have increased 100 percent since the study was conducted in 2010 from 20 percent of organizations reporting criminal attacks to 40 percent of organizations in this year's study.

Employee negligence is considered the biggest security risk. Seventy-five percent of organizations say employee negligence is their biggest worry followed by use of public cloud services (41 percent), mobile device insecurity (40 percent) and cyber attackers (39 percent).

BYOD usage continues to rise. Despite the concerns about employee negligence and the use of insecure mobile devices, 88 percent of organizations permit employees and medical staff to use their own mobile devices such as smart phones or tablets to connect to their organization's networks or enterprise systems such as email. Similar to last year, more than half of organizations are not confident that the personally-owned mobile devices or BYOD are secure.

Heavy use of cloud services increases. As discussed above, healthcare organizations view the use of public cloud services as a serious threat. In fact, only one-third are very confident or confident that information in a public cloud environment is secure. Despite the risk, 40 percent of organizations say they use the cloud heavily, an increase from 32 percent last year. The applications or services most used are backup and storage, file-sharing applications, business applications and document sharing and collaboration.

Half of healthcare organizations are compliant with the post-incident risk assessment requirement in the Final Rule. Fifty-one percent of respondents said they are in full compliance while 49 percent report they are not compliant or are only partially compliant. Thirty-nine percent say their incident assessment process is not effective and cite a lack of consistency and inability to scale their process as the primary reasons.

Healthcare organizations don't trust their third parties or business associates with sensitive patient information. Seventy-three percent of organizations are either somewhat confident (33 percent) or not confident (40 percent) that their business associates would be able to detect, perform an incident risk assessment and notify their organization in the event of a data breach incident as required under the business associate agreement. The business associates

they worry most about are IT service providers, claims processor and benefits management. Only 30 percent are very confident or confident that their business associates are appropriately safeguarding patient data as required under the Final Rule.

Organizations rely on policies and procedures to achieve compliance and secure sensitive information. Fifty-five percent of organizations agree they have the policies and procedures that effectively prevent or quickly detect unauthorized patient data access, loss or theft. Unfortunately, the budget, technologies and resources needed to safeguard patient information from a data breach are not as available. Further, less than half (46 percent) of organizations have personnel who are knowledgeable about HITECH and states' data breach notification laws.

Majority of organizations say the HIPAA Final Rule has either not affected patient data privacy and security programs or it's too early to tell. The HIPAA Final Omnibus Rule seeks to better protect patients by removing the harm threshold. Covered entities and their business associates must still conduct an incident risk assessment, for every data security incident that involves PHI. Rather than determine the risk of harm, the risk assessment determines the probability that PHI has been compromised. While 44 percent of organizations say it has affected their programs, 41 percent say it has not and 15 percent say it is too early to tell. The biggest change has been to require policies and procedures to be updated.

Most healthcare organizations are not in compliance with AOD requirements. Less than half of the organizations in this study report they are in full compliance (25 percent) or nearly in full compliance (23 percent) with the Accounting of Disclosures (AOD) requirement. These organizations say they achieve compliance mostly by an ad-hoc process (31 percent), a paper-based process or tool that was developed internally (27 percent), a software-based process or tool that was developed internally (27 percent) or a software-based process or tool that was developed by a third party (15 percent).