scrypt

Healthcare providers' attitudes towards HIPAA compliance in 2015

Created July, 27 2015

Healthcare providers' attitudes towards HIPAA compliance in 2015

Over the course of this last year the healthcare industry has endured nearly 150 data breaches involving 500 or more individuals[1], with the largest incident affecting a staggering 4.5 million people. HIPAA (The federal Health Insurance Portability and Accountability Act of 1996) violations also reported to be on the rise throughout 2014, with some significant breaches making headlines; most notably, a record breaking $4.8 million settlement occurring as a result of a joint HIPAA breach involving the New York-Presbyterian Hospital and Columbia University.[2]

In response to the significant number of breaches being reported over the past year, Scrypt, Inc. conducted a survey of 769 healthcare providers[3], to examine their attitudes towards HIPAA compliance within their organization, and the healthcare industry in general.

Coincidentally, this survey coincided with Ponemon Institute's Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data[4] - a study that provides comprehensive insights into the privacy and security of healthcare data in the US.

Interestingly, both studies revealed that when it came to individuals' biggest concerns around data security, employee negligence came out on top. While human error is the biggest concern, criminal attacks are now the number one cause of data breaches in the healthcare industry, having increased by 125% in the last 5 years[4].

Despite the volume and severity of recent published data breaches, only one in ten respondents say their organization's HIPAA compliance policies had been affected as a result.

While this is somewhat contradictory to the Ponemon findings, which revealed that 90% of healthcare organizations have experienced a data breach of some kind, Scrypt, Inc.'s findings also revealed that the vast majority of organizations are investing in HIPAA compliant software to exchange ePHI (Electronic Protected Health Information), as well as conducting staff training and user audits in order to minimize breaches. Evidently though, this is still not enough.

When considering the questions for this survey, we felt it was important to draw attention to the Health and Human Services' Office of the National Coordinator for Health Information Technology (ONC)'s 10-year goal for nationwide interoperability[5] for electronic health records (EHR). The findings revealed a lack of confidence with the ONC's goal, as only one in five respondents said they were very confident that interoperability will become a reality.

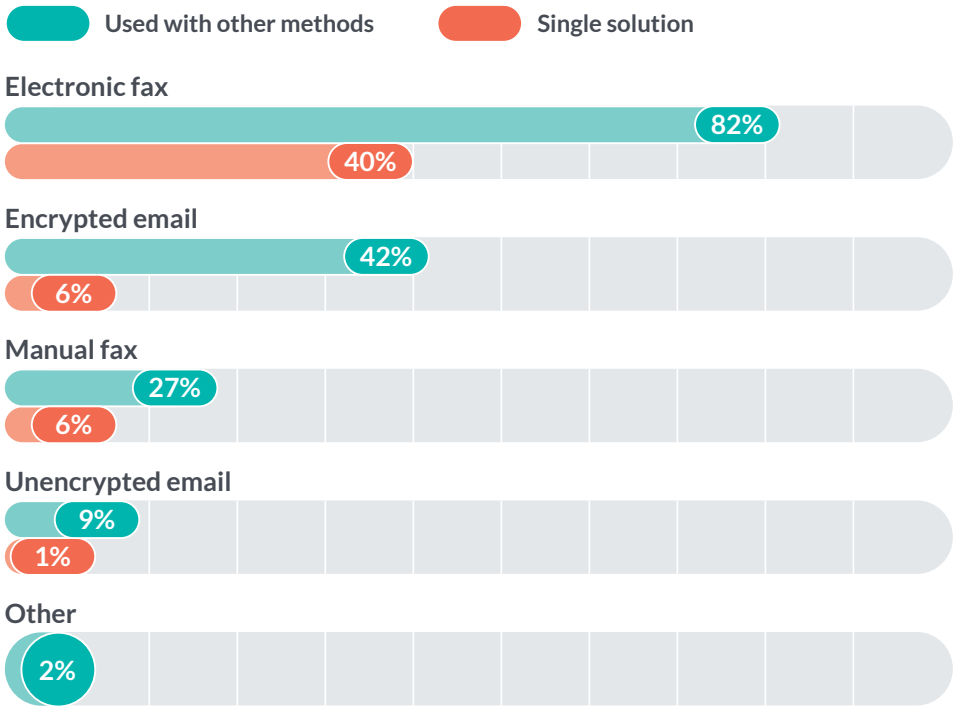
For years the Federal Government has been working hard to protect patient privacy through HIPAA. However, we now live in a world where data is a commodity and protected health information is now 10 times[6] more valuable than financial data on the black market. With this in mind, healthcare organizations are increasingly targeted by data thieves.

With healthcare organizations more vulnerable than ever, they must ensure they are doing everything in their power to protect PHI against malicious attacks, as well as accidental disclosure or loss. While protecting patient privacy should always be the primary concern, a HIPAA violation can have major repercussions on an organization, both in terms of cost and reputation.

[1] https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
[2] http://www.modernhealthcare.com/article/20140507/NEWS/305079946
[3] Sample consisted of existing Sfax customers
[4] https://www2.idexpertscorp.com/fifth-annual-ponemon-study-on-privacy-security-incidents-of-healthcare-data
[5] http://www.healthit.gov/sites/default/files/ONC10yearInteroperabilityConceptPaper.pdf
[6] http://www.reuters.com/article/2014/09/24/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924

Question & Answer

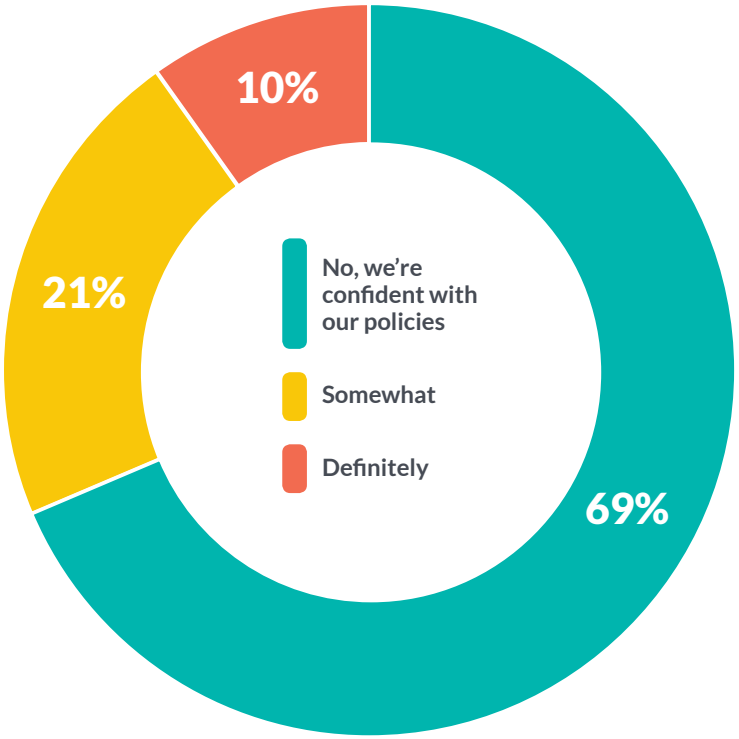
Q1 How is your practice currently exchanging PHI (Protected Health Information) outside of its EHR (Electronic Health Records) / EMR (Electronic Medical Records) or practice management software?



Electronic (cloud) fax continues to be the universal technology for exchanging PHI outside of an organization's' EHR. However, a third of healthcare organizations are using either manual fax or unencrypted email to exchange PHI. This is alarming as both of these methods are inherently insecure and leave information wide open to loss, malicious attack or theft.

Cloud faxing and/or sharing documents within a secure document platform are the only truly secure ways to exchange PHI outside of EMR (Electronic Medical Records) and therefore healthcare organizations and other covered entities should invest in software solutions that are HIPAA compliant to send, receive, or store PHI on any device.

Q2 Have recently publicized breach cases affected your HIPAA compliance policies?



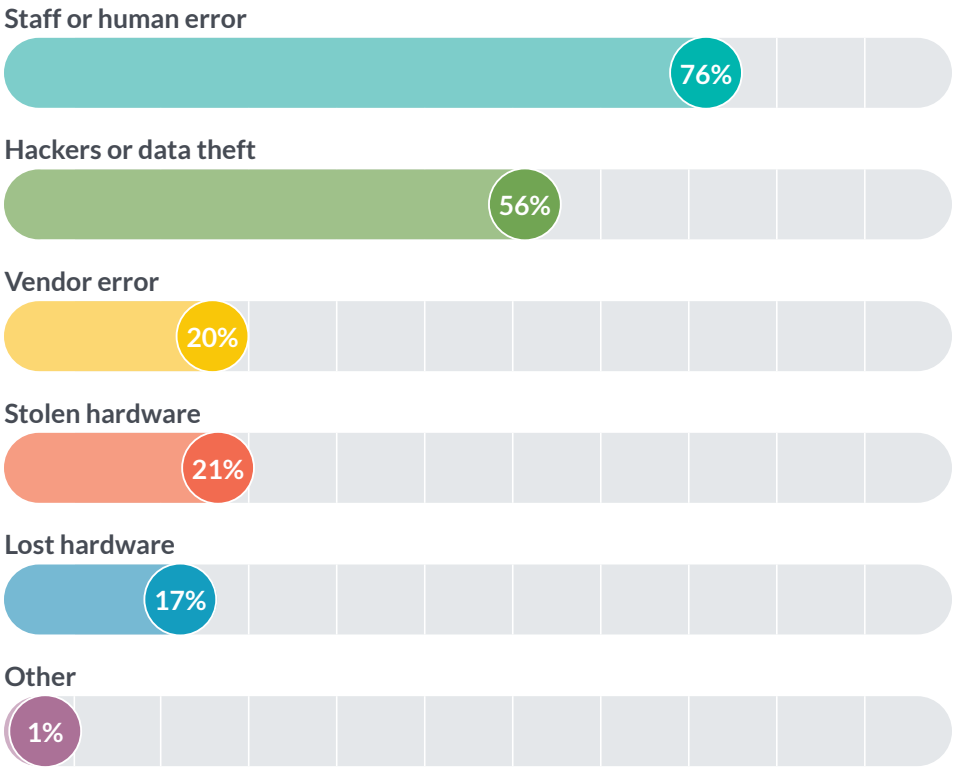
Only one in ten respondents say their organization's HIPAA compliance policies had been affected by recently publicized breach cases. This is perhaps surprising when you consider the findings from Ponemon Institute's Fifth Annual Benchmark Study on Privacy and Security of Healthcare Data, which revealed that over 90% of healthcare organizations have experienced a data breach of some kind.

It is somewhat disconcerting that there isn't a more robust incident response culture and perhaps more worrisome is the seeming lack of preparation of preventing an attack before it happens.

This reinforces the need for healthcare organizations and other covered entities to invest in regular HIPAA compliance training for their staff at every level of their business, and undertake regular reviews of changes to HIPAA policies and procedures.

Another would be to also send internal reminders to employees on a regular basis about security or exposing PHI etc. outside of normal training.

Q3 Who do you feel poses the greatest threat in terms of a HIPAA breach?



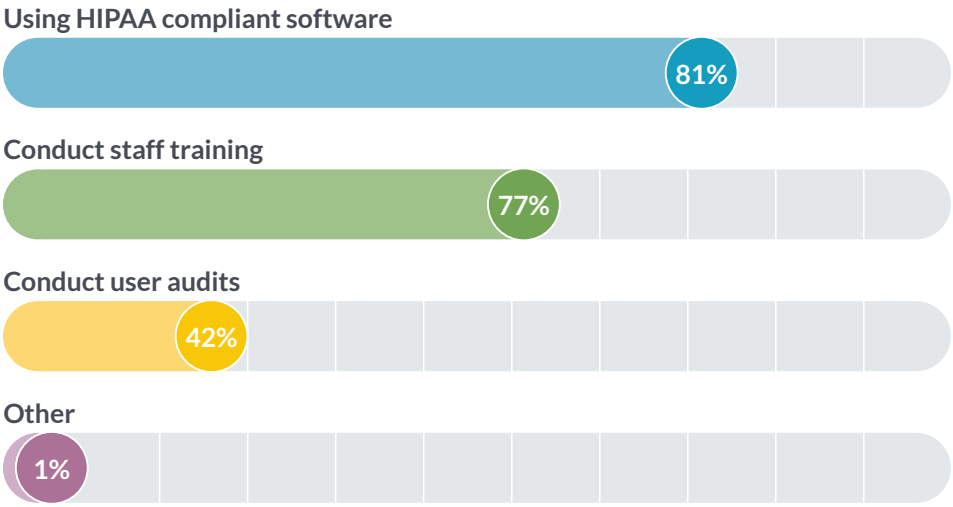
The findings revealed that "staff or human error" is the biggest concern in terms of a potential HIPAA breach within healthcare organizations. This supports the findings from the Ponemon study, which revealed "employee negligence" to be the biggest concern among healthcare organizations when it comes to exposing patient data.

While "human error" is the biggest concern, "criminal attacks" are now the number one cause of data breaches in healthcare, having increased by 125% in the last 5 years.

According to the Ponemon's findings, the average cost of a data breach for healthcare organizations is estimated to be more than $2.1 million. No healthcare organization, regardless of size, is immune from a data breach, yet despite this, half of all organizations have little or no confidence in their ability to detect all patient data that is lost or stolen.

Due to its personal nature, healthcare data represents a higher value than the likes of credit information, for example, which makes the healthcare industry vulnerable, to cyber criminals.

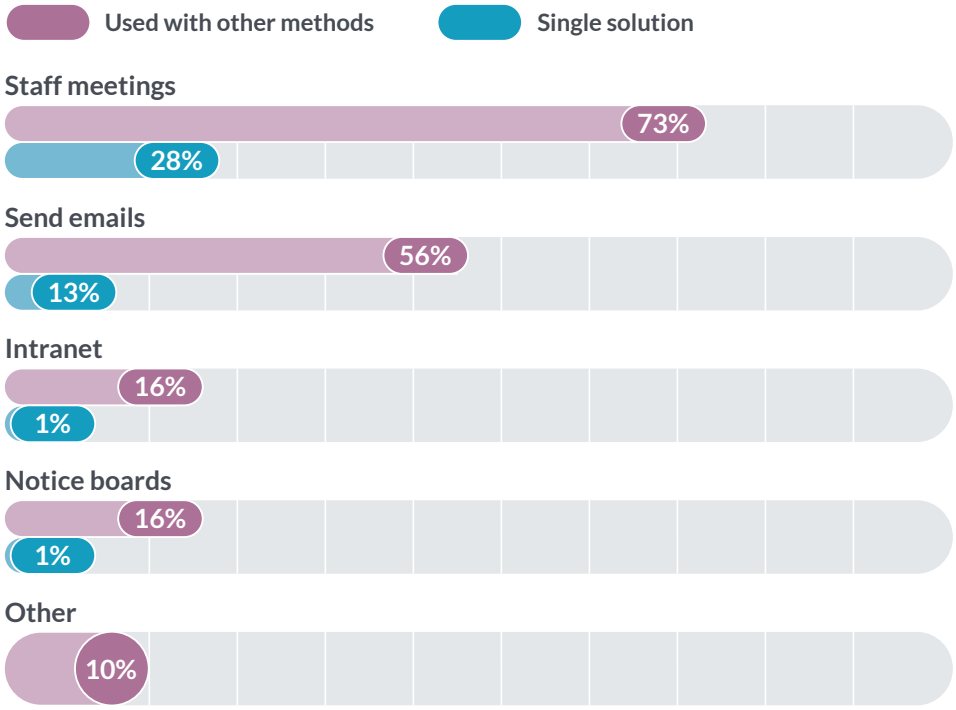
Q4 What is your practice doing to prevent HIPAA breaches?



When it comes to data breaches, prevention is always better than cure, and therefore organizations should be doing all they can to eliminate threats at every level of their business before they come to fruition. While the majority (81%) of respondents are using HIPAA compliant software as a way of protecting patient data, approximately one in five are not.

Even those who are using HIPAA compliant software should be careful, because not all software providers are as secure and robust as they claim to be. To ensure software is HIPAA compliant, Scrypt, Inc. recommends that users conduct regular internal testing of permissions on users accounts, as well as ensuring software partners provide user audit trail reporting.

Q5 How does your organization keep staff informed about changes in HIPAA compliance?

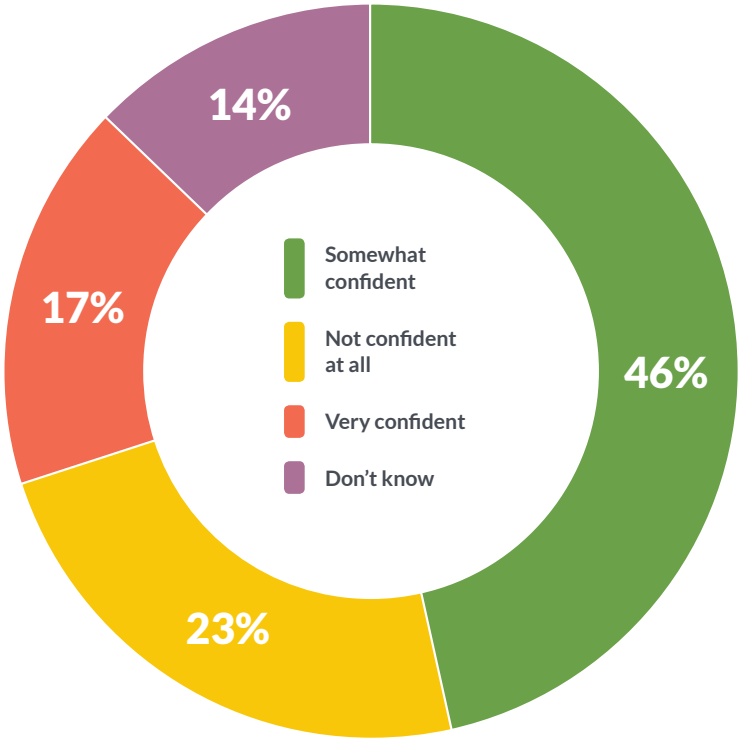


The fact that face-to-face meetings are the most popular form of communication internally is encouraging, as the complex nature of HIPAA compliance is always best communicated and understood in this forum, rather than via email, for example.

There are several sites that offer reliable compliance related information as well as updates on regulations, the most reliable of which is HHS.gov. Larger organizations in particular, that have the budget and resources available to them, have no reason to not keep their employees up to date, as there are several cost effective solutions available through dedicated vendors.

While meetings are an effective way of training staff, HIPAA training should not be a one-off event, but an on-going practice; HIPAA compliance should be engrained in every healthcare organization.

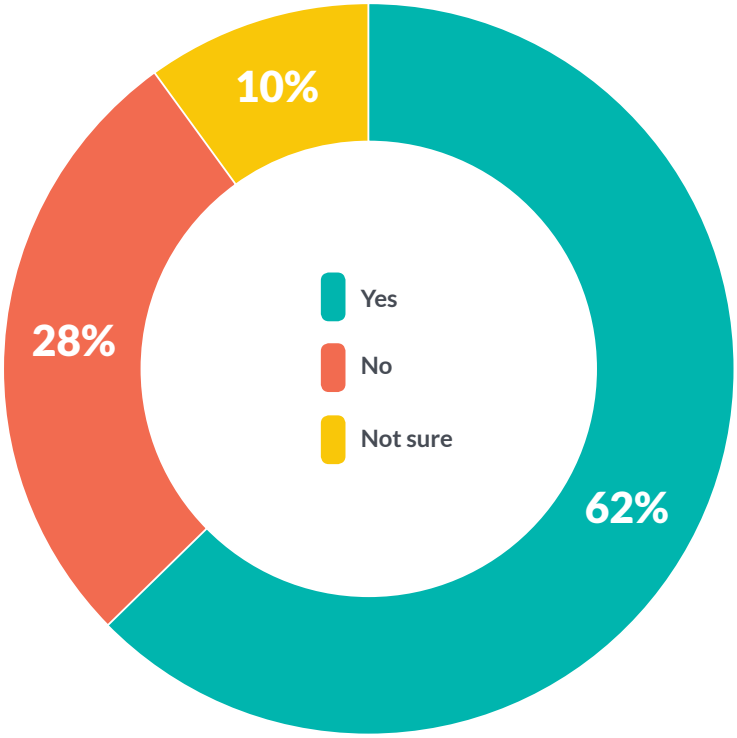
Q6 **The HHS Office of the National Coordinator for Health Information Technology (ONC) has set a 10 year goal for nationwide interoperability. The vision is that by year 10, the nation's health IT infrastructure will support better health for all through a more connected healthcare system and active individual health management. Information sharing will be improved at all levels of public health, and research will better generate evidence that is delivered to the point of care. How confident are you that all providers i.e. the industry as a whole will meet this goal?**



There is evidently a lack of confidence regarding this statement, despite the ONC's confidence. The concept of opening up IP and data sharing among competitors hasn't been widely embraced by EHR vendors, making it difficult to exchange PHI securely outside of non-interoperable systems. Healthcare providers are already using alternative methods to exchange PHI - as was pointed in question number one.

"It will take time to build a fully interoperable infrastructure of coordinated care and communication across healthcare providers, patients and public health entities that improves healthcare quality, lowers healthcare costs and improves population health," the paper's authors said. "No one person, organization or government agency alone can realize this vision of an interconnected health system." (Source: FierceHealthIT)

Q7 Do you think more money from HIPAA fines should be reinvested in improving patient data security?



The majority of respondents believe that more money from HIPAA fines should be reinvested in improving patient data security. Around a third of respondents answered "Not sure", which may suggest they do not know what happens to the fines currently.

According to information available at Federal level, money accumulated from HIPAA fines is channelled back into the Office for Civil Rights, to fund further onsite audits, and to pay the people conducting those audits (some of this is most likely funneled down to the State Attorney General offices in each state as they are the ones actually conducting the audits).

While big fines act as an effective warning to others, they do not solve the problem at its core. Therefore it could be argued that money collected from HIPAA fines would be best invested in improving the security and safety of patient data by informing companies and individuals about protecting PHI data securely.