Finding a Cure for Medical Identity Theft

A look at the rise of medical identity theft and what small healthcare organizations are doing to address threats

October 2014

www.csid.com

TABLE OF CONTENTS

SUMMARY

In 2013, the healthcare industry experienced more data breaches than ever before, accounting for 43% of all breaches for the calendar year. According to Ponemon Research, in 2013 medical identity theft impacted 1.84 million Americans with the average victim being held liable for more than $18,600 in medical services. This includes costs associated with identity protection, legal counsel, medical services because of lapse in healthcare coverage and reimbursements to healthcare providers to pay for the fraudulent services.

While stories about large-scale financial and retail breaches already making headlines, medical identity theft is the next issue to take center stage.

There are two main factors driving the growth of medical identity theft. The first is the value of a medical identity. According to the World Privacy Forum, a medical identity, including name, address, Social Security and health ID numbers, goes for $50 on the online black market. A Social Security number currently sells for $1 and an active credit card can sell for $3. Medical identity theft presents a lucrative source of income for fraudsters.

The second factor driving the growth of medical identity theft is legislative efforts underway that will ultimately enforce the storage of medical records online. Legislation known as The American Recovery and Reinvestment Act (ARRA) calls for the "meaningful use" of electronic health records (EHRs) for all patients in 2014. Starting in 2015, healthcare facilities not showing meaningful use could be penalized. This deadline has many facilities scrambling to get paper systems online, often times before putting policies and security measures in place. Two recent healthcare breaches exemplify how risks will rise as patient data continues to go digital:

- **Community Health Systems**: In August, Community Health Systems, a large healthcare group with 206 hospitals in 29 states, suffered a cyber attack that resulted in the theft of Social Security numbers, names, addresses and phone numbers for 4.5 million patients. This was the largest breach in the U.S. since the Department of Health and Human Services began tracking healthcare breaches in 2009.

- **Healthcare.org:** In July, a hacker broke into part of the Healthcare.org insurance enrollment site and uploaded malware. The malware was uploaded to a server that did not host any sensitive information. While no patient data was taken this time, the breach did raise concerns over how easily the hacker gained access to Healthcare.org.

While stories about large-scale financial and retail breaches already making headlines, medical identity theft is the next issue to take center stage.

With medical identity theft slated to grow as the medical world moves online, CSID conducted a survey to see how healthcare organizations are approaching the issue and what these organizations are doing to mitigate its impact. CSID surveyed 105 healthcare organizations. The majority of respondents were from smaller healthcare organizations with fewer than 5,000 patients including doctors offices (51%), followed by hospitals (16%) and community health centers (4%). Key findings, graphs, charts and takeaways will focus on conclusions gleaned from survey results.

This report is intended to provide a more detailed look into how small healthcare facilities approach patient data security and the actions they take to protect it. This report also presents recommendations on best practices consumers and healthcare organizations should implement to limit the risk and impact of medical identity theft.

KEY FINDINGS

85% of healthcare organizations feel their systems adequately limit the risk of breach

17% of healthcare organizations are worried or very worried about losing patient data in a breach

41% of healthcare organizations spend 10% or less of their IT budget on protecting patient data against breach

50% of healthcare employees who have access to patient EHRs also have access to their personal email at work

32% of healthcare organizations use multi-factor authentication to access sensitive information

GRAPHS & CHARTS

BASICS

A QUARTER OF HEALTHCARE ORGANIZATIONS ARE NOT USING EHRS DESPITE THE 2014 MANDATE.

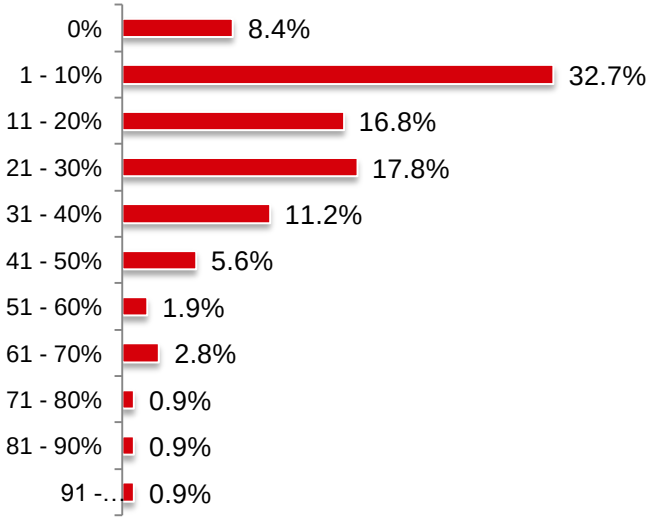
Nearly 26% of respondents say they don't use EHRs. More than a third (37%) have started using EHRs within the past three years, with 11% doing so within the past year.

THE NUMBER OF YEARS HEALTHCARE ORGANIZATIONS HAVE IMPLEMENTED ELECTRONIC HEALTH RECORDS

THE MAJORITY OF SURVEYED HEALTHCARE ORGANIZATIONS SPEND LESS THAN 10% OF THEIR IT BUDGET ON SECURING PATIENT DATA.

An alarming 8% of respondents didn't spend any money on securing patient data. Only 8% of respondents spent more than half of their IT budget on securing patient data.

THE PERCENTAGE OF IT BUDGETS THAT HEALTHCARE ORGANIZATIONS SPEND ON SECURING PATIENT DATA

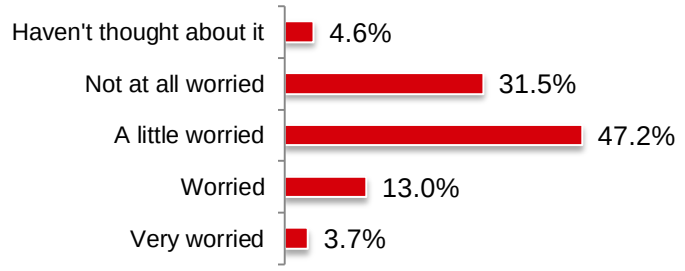


CONCERN

NEARLY A THIRD OF RESPONDENTS ARE NOT WORRIED ABOUT LOSING PATIENT DATA IN A BREACH OR HACK.

Only 17% are worried or very worried about losing patient data. Most are at least thinking about the consequences of a breach or hack with 47% responding they are a little worried.

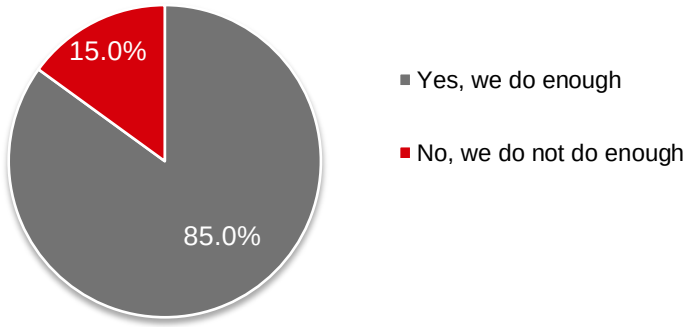
HOW WORRIED HEALTHCARE ORGANIZATIONS ARE ABOUT LOSING PATIENT DATA IN A BREACH OR HACK



ALTHOUGH MOST REPORTED BEING AT LEAST A LITTLE WORRIED ABOUT LOSING PATIENT DATA, THE MAJORITY FEEL THEY DO ENOUGH TO LIMIT THIS RISK.

A whopping 85% of respondents feel that their systems, policies and procedures are enough to adequately limit the risk of breach and hack.

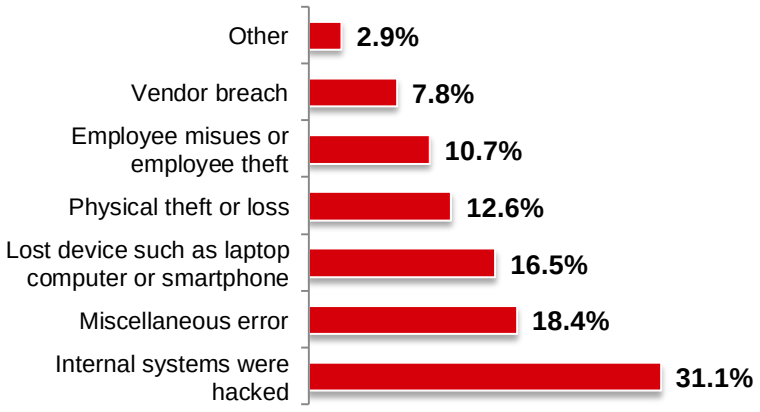
THE PERCENTAGE OF HEALTHCARE ORGANIZATIONS THAT FEEL THEY DO ENOUGH TO LIMIT RISK OF BREACH OR HACK



NEARLY A THIRD OF HEALTHCARE ORGANIZATIONS REPORTED BEING MOST CONCERNED ABOUT INTERNAL SYSTEMS BEING HACKED.

When asked which of the following data loss-related threats they were most concerned about, 31% reported internal systems being hacked, 18% reported data loss via miscellaneous error and 17% reported data loss via a lost device like a laptop.

THE MAIN CONCERNS OF HEALTHCARE ORGANIZATIONS REGARDING BREACHES AND HACKS

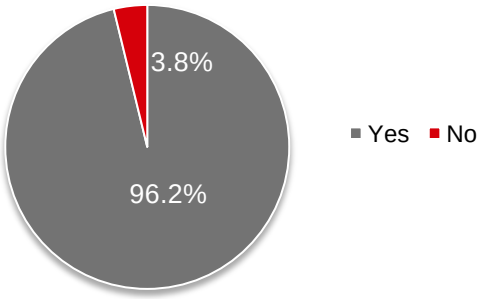


ACTION

THE MAJORITY OF HEALTHCARE ORGANIZATIONS CONTROL ACCESS TO PATIENT RECORDS AND EHRS.

96% reported that they control access to who has access to EHRs.

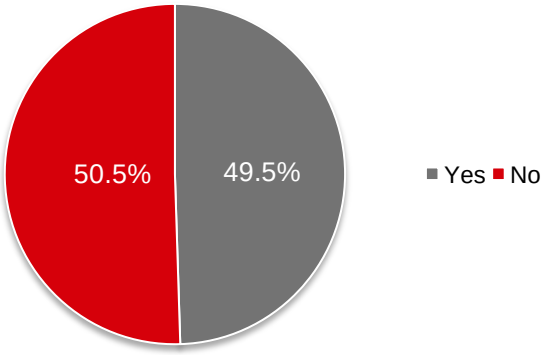
HEALTHCARE ORGANIZATIONS THAT CONTROL ACCESS TO PATIENT ELECTRONIC HEALTH RECORDS



HALF OF EMPLOYEES THAT HAVE ACCESS TO EHRS ALSO HAVE ACCESS TO THEIR PERSONAL EMAIL AT WORK.

Limiting access to personal email in the workplace is a security best practice, and having access to personal email within a healthcare organization makes it easy for patient data to leave a controlled environment undetected.

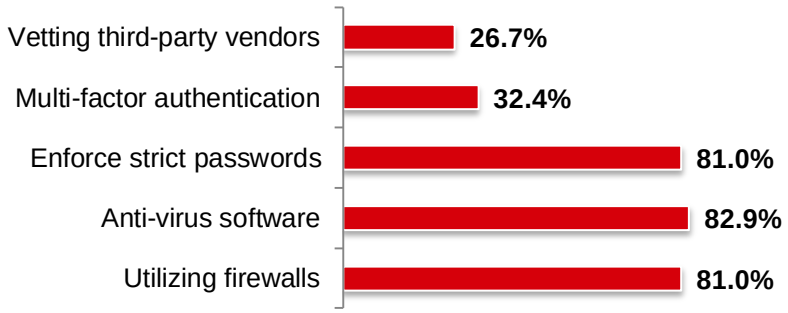
HEALTHCARE EMPLOYEES WITH ACCESS TO EHRS THAT ALSO HAVE ACCESS TO PERSONAL EMAIL AT WORK



HEALTHCARE ORGANIZATIONS ARE GOOD AT IMPLEMENTING BASIC SECURITY MEASURES, BUT HAVE ROOM TO GROW AROUND OTHER BEST PRACTICES.

Respondents seem to have basic security measures down such as utilizing firewalls (81%), maintaining anti-virus software (83%) and enforcing strict passwords (81%) but when it comes to more advance stuff like utilizing multi-factor authentication (34%) and vetting third-party vendors (27%), healthcare organizations have a lot of room to grow.

SECURITY PRACTICES CURRENTLY BEING IMPLEMENTED



TAKEAWAYS

Survey results reveal that there is an opportunity for small healthcare organizations to enhance security procedures and in turn, help protect patient data. In fact, survey results show that many smaller facilities are not implementing security best practices at all. Only 32% of respondents are using multi-factor authentication to secure systems hosting sensitive information, and 48% don't password-protect, encrypt and track mobile devices that host patient data. In one of the most alarming survey findings, only half (50%) of healthcare organizations prohibit access to personal email at work for those that have access to patient EHRs. Limiting access to personal email is a security best practice because access to personal email in the workplace makes it easy for patient data to leave a controlled environment undetected. This is a dangerous practice, even if that patient data is being emailed for non-malicious reasons such as a physician wanting to take a look at a patient's records while at home or traveling.

One would assume that smaller healthcare facilities would lag behind when it comes to security, as large hospitals have greater access to resources and larger IT teams. But alarmingly, survey results show that these smaller facilities overwhelmingly feel their patient data is secure (85%). However, there is a huge disconnect between this perceived security and their actual implementation of EHR security best practices. For example, other security best practices not being implemented by these smaller healthcare facilities include:

- 73% of respondents don't vet and audit vendors that have access to sensitive information
- 44% don't have regular employee education around security best practices
- 73% do not have a response plan in place in the event that patient information is lost

It should be noted that most small healthcare organizations are implementing the basics, such as using anti-virus software (83%), enforcing strict password guidelines (81%) and hosting sensitive information behind a firewall (81%). The majority of healthcare organizations (96%) also limit employee access to EHRs based on their roles within the healthcare organization. For example, a nurse will need access to patient health records for treatment; a billing technician does not.

So what can be done to ensure patient security?

To begin, smaller healthcare organizations need to devote a larger portion of IT budgets to EHR security. Out of the 105 survey respondents, only 13% said they spend more than 41% of their IT budget on security-related IT. A whopping 41% spend less than 10% on security with 8% of those respondents claiming they spend nothing at all on securing patient data from breach.

While there is no industry benchmark on what percentage healthcare organizations should devote to protecting their systems, experts from the industry group, Medical Identity and Fraud Association (MIFA) recommend it should be more than 10%.

Another key area where healthcare organizations need to focus security efforts is securing patient data on mobile devices. Just last year, Seton Healthcare Family lost medical data for 5,500 patients after a laptop with unencrypted patient information was stolen from an employee's car. Putting security policies and procedures in place to secure mobile devices, especially as bring your own device (BYOD) continues to grow in popularity, will be absolutely essential to securing patient data moving forward.

Overall, the survey demonstrates that while healthcare organizations may perceive their patient data to be safe, security best practices are not being implemented. There is room for growth when it comes to employee education, securing mobile devices, vetting third party vendors, utilizing multi-factor authentication and implementing the other security best practices that are further outlined in the below tips section. To learn more about medical identity theft and CSID's survey results, watch CSID's cyberSAFE webinar titled "Finding a Cure for Medical Identity Theft" at www.csid.com/medicalIDtheft.

RECOMMENDATIONS

SECURITY BEST PRACTICES FOR HEALTHCARE ORGANIZATIONS

Keep up with the basics. Utilize best password practices, install and maintain anti-virus software, and ensure all sensitive data is behind a firewall.

Track, encrypt and password-protect mobile devices hosting patient information. Create a BYOD policy that puts strict limits on how patient data can be viewed and transmitted on devices.

Educate your employees. Educate employees on how medical identity theft happens, what are the warning signs, and what they need to do from a best practices standpoint and a HIPAA standpoint to keep patient data safe.

Use multi-factor authentication. Use multi-factor authentication to secure systems hosting patient data.

Audit third party vendors. Audit all third party vendors that have access to or host patient information.

Implement role-based security access to patient records. Role-based security access ensures HIPAA compliance and reductes the risk of litigation in the event that patient data is lost.

Create an identity theft crisis response plan. Maintain the plan by keeping it up-to-date and train staff on relevant policies and procedures.

Collaborate with other healthcare organizations. Learn from others and share resources in an closed environment.

SECURITY BEST PRACTICES FOR CONSUMERS*

Review your Explanation of Benefits (EOBs). Ensure the doctors listed and services provided are accurate. If you find an incorrect item, even if no money is owed, contact your insurance company immediately.

Obtain your "benefits request" annually. Your insurance provider can provide a list of all benefits and services paid in your name, which you can review to confirm all the services listed were received.

Protect your medical insurance card. Leave your insurance card in a safe place, and don't carry it with you unless it's necessary.

Safeguard your insurance-related paperwork. Shred or file your EOBs in a safe, and preferably locked location.

Report lost or stolen health insurance identification cards. Alert your insurance carrier of misplaced, lost or stolen cards to avoid unauthorized use.

Use vigilance when providing your personal or insurance information. Be sure you're dealing with a reputable healthcare provider. Be cautious when offered free medical services. Often fraudsters use this as a way to obtain your health information.

Review your credit reports annually. You have a right to request a free annual credit report from each of the three credit bureaus. Be sure your reports are free of any medical liens. Reviewing your medical record is a little more tricky and time-consuming but it is a good practice if your personal information has even been part of a data breach, your financial informaiton has been compromised or if you have seen any warning signs that your medical identity may have been compromised.

*Source: Medical Identity Fraud Alliance

METHODOLOGY

CSID and digital data collection firm Research Now teamed up to survey a demographically representative sample of 105 security decision makers at healthcare organizations in the U.S.

ABOUT CSID

CSID is the leading provider of global identity protection and fraud detection technologies and solutions for businesses, their employees, and consumers. With CSID's advanced enterprise-level solutions, businesses can take a proactive approach to protecting the identities of their consumers all around the world. CSID's comprehensive identity protection products advance from credit monitoring to include a full suite of identity monitoring services; insurance and full-service restoration; identity authentication and voice biometrics; and proactive breach mitigation and resolution.

www.csid.com

ABOUT RESEARCH NOW

Research Now, the leading digital data collection provider, powers market research insights. They enable companies to listen to and interact with the world's consumers and business professionals through online panels, as well as mobile, digital and social media technologies. Their team operates in 24 offices globally and is recognized as the market research industry's leader in client satisfaction. They foster a socially responsible culture by empowering our employees to give back.

www.researchnow.com