resolution

your client's identity at risk. our solutions at work.™

# A Look at Medical Identity theft. It's not great news…

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.

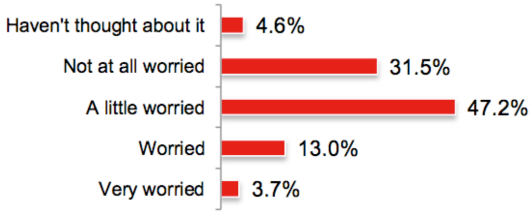
There are two main factors driving the growth of medical identity theft. The first is the value of a medical identity. According to the World Privacy Forum, a medical identity, including name, address, Social Security and health ID numbers, goes for $50 on the online black market. A Social Security number 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.

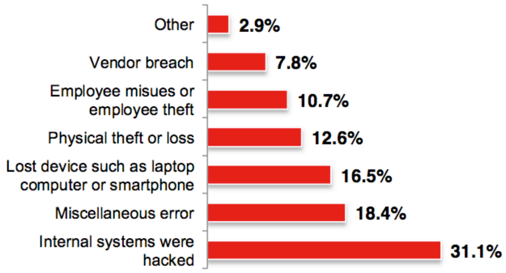
## A QUARTER OF HEALTHCARE ORGANIZATIONS ARE NOT USING EHRS DESPITE THE 2014 MANDATE.

Nearly 26% of respondents in a CSID* study 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.

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



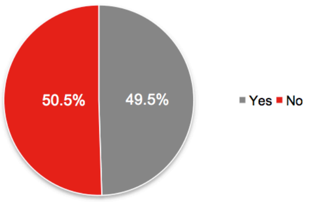
THE MAIN CONCERNS OF HEALTHCARE ORGANIZATIONS REGARDING BREACHES AND HACKS



## FOOD FOR THOUGHT

There is an opportunity for small healthcare organizations to enhance security procedures and in turn, help protect patient data. In fact, the CSID 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.

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



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.

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.

At ID Resolution we have created robust programs to help deal with and mitigate the potential for data breach and identity theft.

Contact us for more information and visit our website at www.idresolution.net

*Source CSID 2014

## About ID Resolution

ID RESOLUTION™ is an innovative, client focused company that provides a full suite of identity management solutions. Formed by people who were at the forefront of the industry created to combat and deal with identity theft, our executives and staff create and customize new products and bring new ideas to satisfy our clients ever changing needs.

Our superior management information and reporting, customer satisfaction testimonials and seamless transitioning to incorporate new products will help you gain more sales, new opportunities and increased customer loyalty.