7 Things About Medical Identity Theft Healthcare Executives Need To Know

iBridge™

7 Things About Medical Identity Theft Healthcare Executives Need To Know

When thinking about identity theft, the picture that most often comes to mind is credit card fraud or unauthorized access to the victim's bank account. However, medical identity theft—the act of stealing someone's health records or other medical information—is quickly climbing the ranks as a threat against the public that may be even more serious ... and one spreading all too rapidly.

While the risks associated with other types of identity theft are obvious, it's harder to see the immediate motivation behind stealing anyone's medical records. The cybercriminal responsible for the crime can benefit in several ways: using the victim's social security number to obtain medical devices or services illegally, filing a fraudulent claim for insurance reimbursements or purchasing (and/or reselling) prescription drugs.

Medical identity theft represents a systemic flaw that could drive healthcare costs up even further and at worst a tragic situation that could cause sickness or death due to inaccurate health records. Here are seven things about medical ID theft that healthcare executives must know to limit the possibility of data breaches within their own organizations.

The expense to the consumer is much higher than with other forms of identity theft; the average cost of medical ID theft in 2013 was $18,660 per victim, with some individuals experiencing damages over $100,000.

1. Medical ID Theft Is on the Rise

Medical identity theft saw a 20 percent increase from 2012 to 2013 alone giving the healthcare industry proof positive that the problem is not going anywhere. The assumption, theft is carried out by some shady figure in the cybercriminal underworld, when it is consumers who put themselves at risk by sharing medical information with friends or family and most security breaches are carried out with the help of someone on the inside.

Since medical identity theft is a multi-billion dollar industry, many hackers see a huge payday from the theft of personal medical information. Health records are a valuable haul because just a single file can deliver everything from a social security number to a patient's health insurance and payment information or even a physical description of the victim.

The expense to the consumer is much higher than with other forms of identity theft; the average cost of medical ID theft in 2013 was $18,660 per victim, with some individuals experiencing damages over $100,000. These costs can be direct, or indirect— having to pay higher premiums due to records indicating a medical condition that doesn't exist or being billed for services that the victim never received and then having those unpaid bills affect credit scores.

Medically-related identity thefts in the United States accounted for nearly half (43 percent) of all reported identity thefts in 2013, or approximately 1.84 million Americans. This total is higher than ID thefts related to the government, the military or banking/ financial services.

2. Medical ID Theft Represents Nearly Half of All identity Thefts in the United States

According to a recent survey from the Identity Theft Resource Center, medically-related identity thefts in the United States accounted for nearly half (43 percent) of all reported identity thefts in 2013, or approximately 1.84 million Americans. This total is higher than ID thefts related to the government, the military or banking/ financial services. Since 2009, the U.S. Department of Health and Human Services tracked personal medical record theft, estimates suggest between 27.8 million and 67.7 million personal records are lost to a breach.

Yet, there does not seem to be a correspondingly high level of consumer education about the potential for medical ID theft, let alone the possible consequences. There is also a staggering lack of education at the executive level.

The wealth of usable data available in a single place makes medical records a valuable target for cybercriminals, with each record commanding between 20 and 50 times more in price than other types of identity record theft could deliver.

3. Medical Records Are Incredibly Valuable to Hackers and Cybercriminals

The wealth of usable data available in a single place makes medical records a valuable target for cybercriminals, with each record commanding between 20 and 50 times more in price than other types of identity record theft could deliver. The sale of medical information to the highest bidder is at a huge profit margin; an entire record sold as a package, or doling out bits of information piecemeal for a profit, just like parting out a stolen car.

Not only can medical data be exploited directly, but the details within healthcare records can be leveraged against other forms of privacy violations, identity theft and fraud. If one of the security questions on the victim's online, banking site asks a question such as "What was the first bone you broke?" to verify the user's identity, this information cross-referenced against personal medical records. Other tidbits of data such as birthdays, children's birth dates, and social security numbers can prove similarly useful to hackers attempting to gain access to other accounts.

Perhaps most chilling is the realization that medical identity theft is rarely a single attack; instead, the victims often suffer repercussions for years to come.

4. Medical Identity Theft Can Put Health and Wellbeing at Risk

Although the financial costs of medical ID theft are undeniably high, the victims' savings account balances are far from being the only thing at risk after a breach. Identity theft puts the health and wellbeing of a patient on the line:

- Incorrect medical data could lead to a patient receiving a transfusion of the wrong blood type or receiving medication to which he or she is actually allergic.

- Altered medical records could lead to incorrect diagnoses or victims failing to receive the treatment they need in a timely manner.

- If stolen data revealed a public figure had, a certain health condition that the victim did not want made public, blackmail could follow.

Perhaps most chilling is the realization that medical identity theft is rarely a single attack; instead, the victims often suffer repercussions for years to come.

5. Victims of Medical Identity Theft Often Have Little to No Recourse after the Fact

With standard identity theft, there are clear steps that victims can take: canceling their credit cards or disputing charges, contacting their banks and disputing incorrect information on their credit reports, to name a few. Yet, the victims of medical ID theft typically find their hands are tied as far as whom they should tell or how they should handle the situation.

Individuals can request to see their medical records, but lack the legal right to request corrections; no single agency that handles such issues. Healthcare practices are not required to correct invalid data in medical records transferred from other practices. Most are reluctant to change records that did not originate from their own practice out of liability concerns. How can those affected by medical ID theft have inaccurate data corrected or removed from their records?

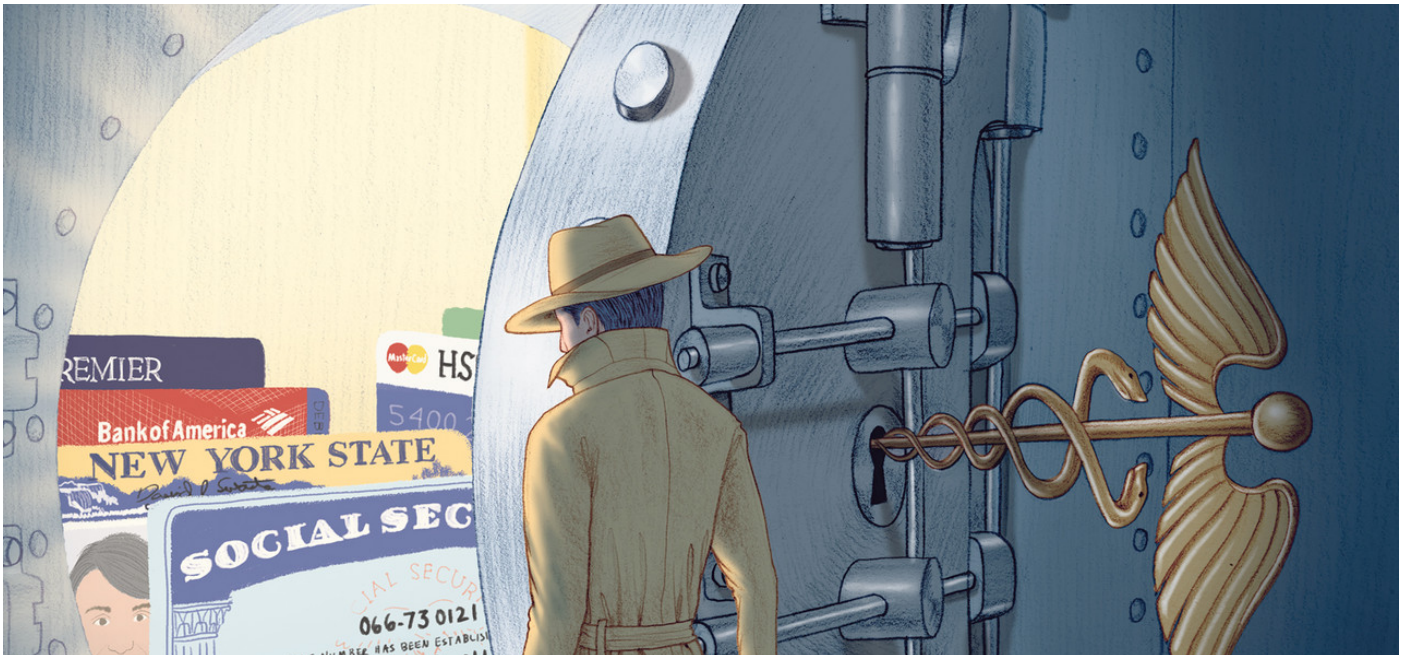
Electronic medical data, if not properly password-protected and encrypted, is simple to download onto a jump drive and then can be transported just about anywhere. Security must start at the top and work its way down through the ranks to limit the potential for this criminal infiltration.

6. Medical Theft Is Under-Researched and Under-Reported

The incidence of medical ID theft is chronically under-reported, has led to the issue being under-researched. Although hard statistics based on reported breaches, listed above; the Federal Trade Commission (FTC) estimates that the real number of those affected by medical identity theft may be as high as three times that amount.

Whether these incidences go unacknowledged due to a lack of awareness by the victim that they've occurred, or those affected just don't know where to report the breach is impossible to say. Yet, that either scenario exists at all is just another indicator that medical identity theft must be more widely recognized as a potential threat by the public.

One factor that's hardest to control is that the most successful medical ID thefts are insider crimes, typically seen in collaboration with an existing employee of the affected organization or at least someone who has access to healthcare records. Electronic medical data, if not properly password-protected and encrypted, is simple to download onto a jump drive and then can be transported just about anywhere. Security must start at the top and work its way down through the ranks to limit the potential for this criminal infiltration.



Ensuring that healthcare organizations are HIPAA compliant drastically reduces vulnerability to consumer and practice.

7. HIPAA Helps

Ensuring that healthcare organizations are HIPAA compliant drastically reduces vulnerability to consumer and practice. From controlling, the way medical data is stored and transmitted to ensuring that only authorized persons can access medical records, following HIPAA guidelines helps protect patient data.

Yet, HIPAA compliance does not guarantee immunity against hackers. There will always be an unpredictable human element in every healthcare practice, so increasing awareness about the dangers and warning signs of medical ID theft among medical and support staff and strictly enforcing data privacy policies must remain top priorities for any healthcare organization.

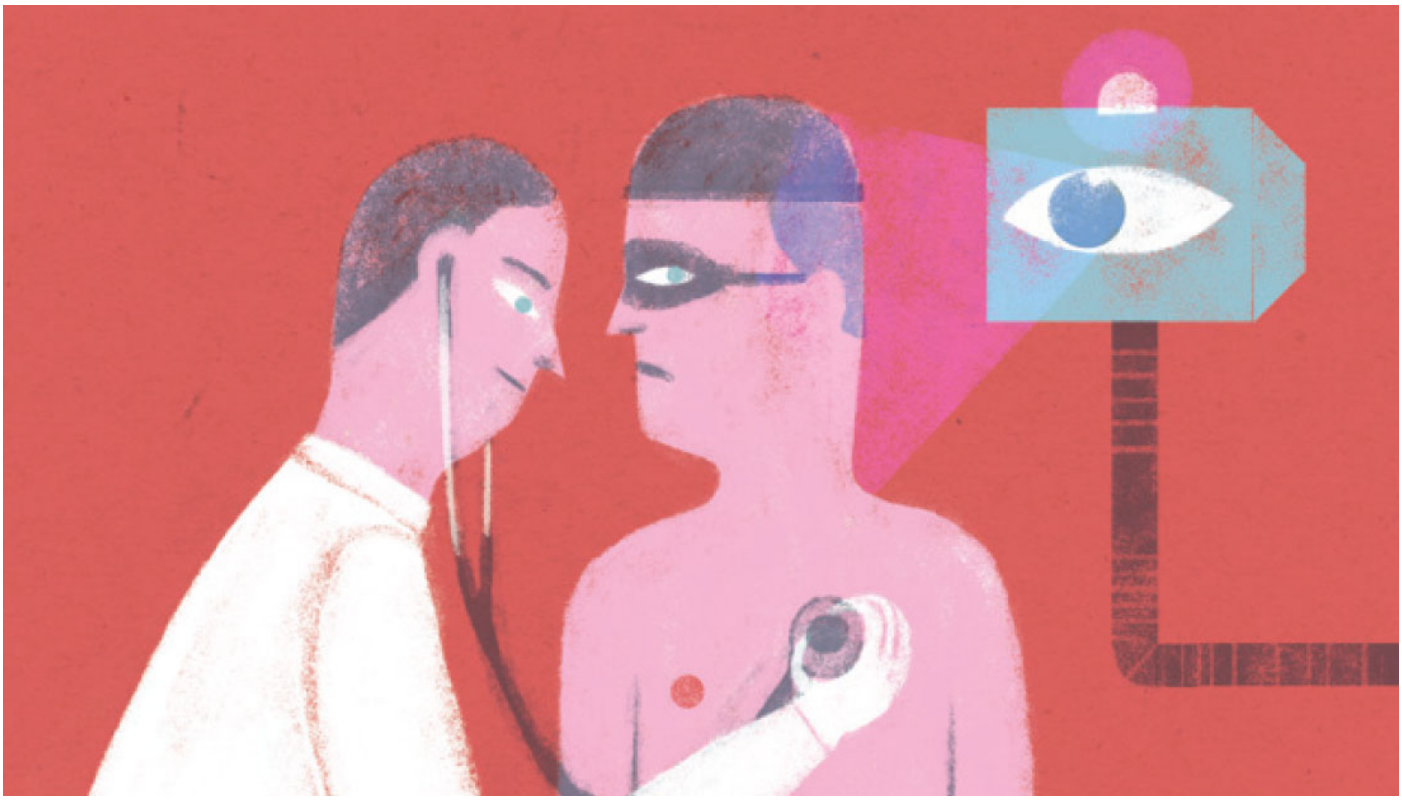
As with nearly any identity theft, the best defense is a good offense. Maintaining HIPAA compliance is vital, as conducting thorough background checks on all medical and support staff and restricting access to sensitive data on a need-to-know basis only.

The Big Picture

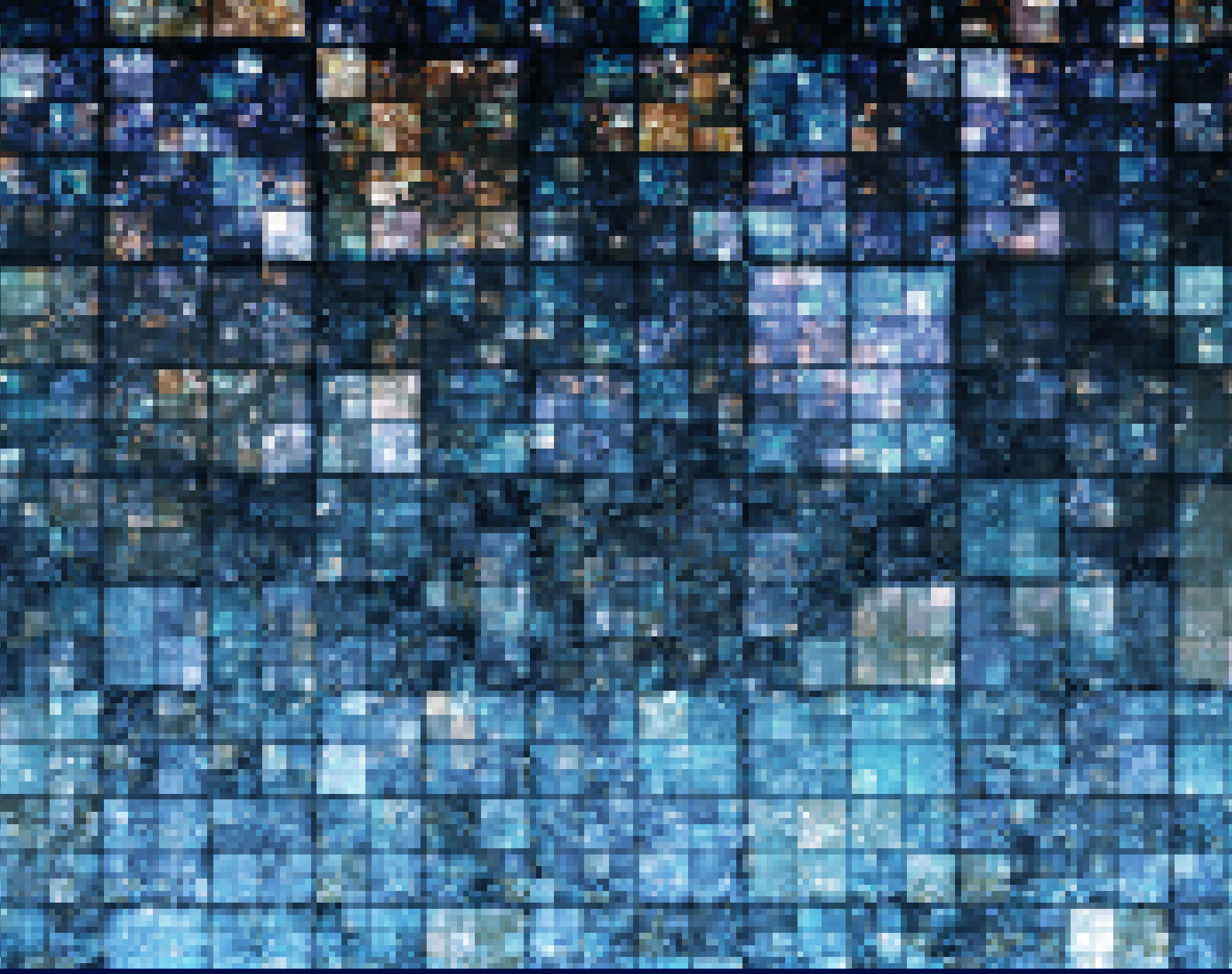
This white paper covers only an overview of the potential ramifications that could occur because of medical identity theft. While the impact to the victims is tremendous, healthcare organizations themselves are also deeply affected. Even worse, the rate of occurrence continues to rise, which translates into higher healthcare costs as practices scramble to implement new policies or install new infrastructure hoping to limit future data breaches.

Unfortunately, decision-makers are not in agreement about who is ultimately accountable for preventing medical identity theft: healthcare practices, consumers themselves or the government. Because of this, there is no single agency responsible for damage control; there is also a distinct lack of standard operating procedures for those affected—whether patient or practice—should follow if a data breach occurs.

As with nearly any identity theft, the best defense is a good offense. Maintaining HIPAA compliance is vital, as conducting thorough background checks on all medical and support staff and restricting access to sensitive data on a need-to-know basis only. As electronic health records increase in number, maintaining data security has become—and will continue becoming—more vital than ever. It is also essential that, as healthcare organizations move forward with any managed services or other hardware and software upgrades, they work only with HIPAA-knowledgeable vendors well versed in the best way to safeguard patient data.



On the grounds of sheer profitability alone, medical identity theft is not going anywhere soon. While healthcare executives may not eradicate these incidences completely, the right combination of awareness and proactivity can better protect the privacy of the patient and help ensure the continued integrity of the healthcare organization itself.



If you would like to learn more about how iBridge can help you with your data security, please contact us.

info@ibridgellc.com
503.906.3930

Follow us!