Medical Identity Theft:
A Deadly Side Effect of Healthcare
Data Breaches
Patients are a vulnerable population. Their health, even their lives, rest in the hands of healthcare providers. Equally vulnerable are patient’s health records. In today’s connected world, this data is strewn across the digital universe. From electronic health records (EHRs) to physician’s iPads to wearable health devices, a patient’s confidential medical information is available to more people in more places than ever before. Sensitive medical diagnoses, health insurance numbers, and other information are there for the viewing — and the stealing.

Thieves love healthcare records. Not only do they fetch a good price on the black market, but medical identity theft is a hot business. This form of identity crime occurs when criminals use patient information to obtain medical goods and services or to receive other financial benefits. Once their records are compromised, patients are at serious risk for misdiagnoses, mistreatment, or other medical mistakes that endanger their health, if not their lives.

Thanks to the growing threat of data breaches that expose and endanger patient information, medical identity theft will only get worse. But there is hope. Understanding the risks and causes of this crime can help you contain it.

In this eBook you’ll:
- Learn the size and scope of medical identity theft.
- Discover how healthcare data breaches turn patients into victims.
- Get the insider view on healthcare fraud.
- Study the thorny issue of identity ownership.

Your patients deserve the best care. They also deserve the best protection against medical identity theft that you can provide. We hope this information helps.

Contents

Forward .................................................. 2
Medical Identity Theft: A Big Deal, or Much Ado About Nothing? ................................. 3
How Healthcare Data Breaches Turn Patients Into Victims ........................................... 5
Unraveling Healthcare Fraud: The Dog That Ate The Evidence .................................. 7
Horcruxes in Healthcare: Who Owns Your Medical Identity? ....................................... 9
Helpful Links & Resources ................................. 12

About This Document
This document is intended to provide you with general information about the risks and causes of medical identity theft. However, the content is not intended to be exhaustive regarding this topic, and is not intended to be or replace expert advice. Please seek legal counsel or your data breach provider for such advice.
The number of Americans whose healthcare information has been disclosed in data breaches — **140,000,000 in the past few years**¹, nearly half of all Americans—is enough to make anyone feel slightly ill. Yet only a percentage have fallen victim to actual medical identity theft, 2.3 million adult patients in 2014, according to the latest Ponemon Institute study on this topic².

So this poses an important question: Is medical identity theft³ that big of a deal?

According to a recent New York Times article, “Stolen Consumer Data Is a Smaller Problem Than It Seems”⁴, the answer is no—at least for identity theft in general. While the author admits to the horrors of identity theft, he noted that “consumers are almost never on the hook for financial losses in these sorts of episodes, which, by the way, have also been on the decline.”

In fact, he wrote, “This relatively sanguine picture of the impact of data breaches is an example of a threat that looks worse than it turns out to be.” The picture is not so sanguine for victims of medical identity theft, however. The number of victims has nearly doubled in five years, according to Ponemon, and the health consequences of this crime will never be cured with credit monitoring, the traditional help offered to victims. In addition, privacy laws, which in some cases appear to protect the thief more than the patient, can cause the problem to drag on for years.

A recent Wall Street Journal article highlights the havoc medical identity theft can have on its victims:

- A man with Down syndrome was billed for a leg-injury treatment that he never received. In addition, his health record was contaminated with the thief’s medical information, including a drug allergy he didn’t have.
- An undocumented immigrant used somebody else’s name to get a liver transplant.
- A retired Florida woman with two feet was billed for an amputated foot.
- A man was unable to fill his legitimate prescriptions because his medical benefits had been “looted.”
Who’s Sounding the Alarm?
The NYT article compared the security firms that provide statistics on identity fraud and online attacks “to the soap company that advertises how many different types of bacteria are on a subway pole without mentioning how unlikely it is that any of those bacteria would make you sick.”

This harsh criticism is not without cause; nonetheless, the problem is very real. The government itself is visibly concerned about medical identity theft. Gary Cantrell, deputy inspector general for investigations at HHS’s Office of Inspector General said in the Wall Street Journal article: “Identity theft is pervasive throughout health care. We see it as a growing concern.”

In addition, President Barack Obama signed a bill that requires the removal of Social Security numbers from Medicare cards by April 2019.

On the state level, Nevada, Oregon, Rhode Island and Connecticut recently updated their consumer notification laws¹ to expand their definition of sensitive personal data to include protected health information (PHI).

We can only hope that healthcare organizations and the government continue to prioritize medical identity theft.

Because for the ever-growing number of Americans whose health is at risk from improper disclosure of their information, medical identity theft is a very big deal, indeed.

Criminals can not only access bank accounts and prescriptions illegally, but they could alter a patient’s data or interfere with ongoing medical procedures — both with life-threatening consequences.”

— Professor Frank Ulrich Montgomery, Vice Chairman, World Medical Association (WMA), DailyMail.com

¹https://www2.idexpertscorp.com/blog/single/half-of-americans-health-information-disclosed-in-data-breaches
²http://medidfraud.org/2014-fifth-annual-study-on-medical-identity-theft/
³https://www2.idexpertscorp.com/midas-software
⁵http://www.lexology.com/library/detail.aspx?g=dc4c229d-110f-4f9b-b32f-d7234c9e866c
How Healthcare Data Breaches Turn Patients Into Victims

By Jeremy Henley, Director of Breach Services

Passengers on the London Underground are told to “mind the gap,” a warning to watch for the space between the train door and station platform. Healthcare organizations need to mind their own privacy and security gaps when it comes to protecting sensitive medical information.

According to the latest Gemalto’s Breach Level Index¹, the healthcare sector had the most data breaches in the first half of 2016, accounting for 27 percent of total incidents across all industries. The nature of these gaps has changed over the years — for instance, criminal attacks are now the leading cause of healthcare data breaches², according to Ponemon Institute’s Fifth Annual Benchmark Study on Privacy & Security of Healthcare Data³. These breaches, particularly those caused by the criminal element, have caused medical identity theft to nearly double in five years⁴.

The Link Between Data Breach and Medical Identity Theft

According to the Wall Street Journal, medical identity theft is on the rise because of the surge in electronic health records and healthcare data breaches. But it’s more than the digitization of health records. Medical data is everywhere, thanks to a plethora of devices, from tablet computers to medical implants and even Fitbits and Apple watches that are recording health data and transmitting it over the Internet.

Rick Kam, president and co-founder of ID Experts, told Forbes⁵ that healthcare data breaches are also on the rise because financial services and retail sectors have developed better strategies for protecting their data. This includes the use of EMV cards that use a chip instead of a magnetic stripe. As a result, many hackers are turning to the more vulnerable healthcare industry.

In addition, he said, medical information is simply more profitable on the black market. The Dark Web⁶ offers cyber-criminals multiple global marketplaces.
in which to sell stolen personal information, including healthcare records.

“This is all converging to create a perfect storm for getting this data,” Rick Kam said in the Forbes article. “It’s more available, it’s worth more, and the healthcare organizations aren’t as good at protecting the data because they haven’t had to be.”

As Dr. Shantanu Agrawal, director of the Center for Program Integrity at the Centers for Medicare and Medicaid Services, told the Journal, “Data breaches are increasing and becoming more common. You can end up with diagnoses being placed in your file without your knowledge.”

Smart, Strategic Data Protection
To protect patients against the harms of medical identity theft, the healthcare sector must step up its data protection measures. While there is no such thing as zero risk in today’s connected, digitized world, health plans, hospitals and other entities that hold medical information can mount a strategic defense against cyber criminals.

For instance, in a MedPage Today interview, Dwayne Melancon, Chief Technology Officer with Tripwire, recommended following the example of financial institutions that classify and segregate their data, limiting access only to those who need it.

Melancon also cautioned healthcare organizations to spend their security dollars wisely. “Just because it’s a dollar spent on security doesn’t mean it’s worth spending,” he says. “All of this should be aligned within a good risk framework to make sure that people really are spending in a way that increases security, and doesn’t just add window dressing.”

In other words, they must mind the gap.

SHARE THIS ARTICLE:

After the 2015 breach of 100 million medical records from Anthem, Premera Blue Cross, and Excellus Health Plan, let alone the numerous smaller networks compromised in 2015 and 2016, the annual rate of medical identity theft could easily increase to be ten or twenty times greater than the 2014 rate.”

— Your Life, Repackaged and Resold: The Deep Web Exploitation of Health Sector Breach Victims
Institute for Critical Infrastructure Technology

3 https://www2.idexpertscorp.com/fifth-annual-ponemon-study-on-privacy-security-incidents-of-healthcare-data
4 http://medidfraud.org/2014-fifth-annual-study-on-medical-identity-theft/
6 https://www2.idexpertscorp.com/blog/single/know-your-enemy-the-new-economics-of-cyber-crime
7 http://www.medpagetoday.com/PublicHealthPolicy/PublicHealth/49914
Unraveling Healthcare Fraud: The Dog That Ate The Evidence

By Rick Kam, President & Co-Founder

In a Glendale, Calif., parking lot, two individuals are burning items in a barrel—paper, maybe, but the surveillance footage supplied by the Wall Street Journal is unclear.

In another video clip, the same parking lot is crammed with minivans and people, elderly or homeless patients who are given bogus or superficial exams at the Manor Medical Imaging Clinic. It’s what prosecutors call a “typical day at the clinic.”

Using these patients’ identities, fraudsters filed false claims for costly antipsychotic medications, which they would sell on the black market. According to the Wall Street Journal, the clinic filed nearly 8,500 claims, costing Medicare and California’s Medi-Cal a total of $4.5 million during a six-month surveillance period. Authorities made arrests in 2011, and in 2014 three people including a physician were convicted for their roles in the $20 million scheme.

Healthcare fraud cases such as this one read like a cheesy detective novel (remember the motorized scooter debacle from a few years back?), but they are not fiction and they are all too common. Statistics vary, but The Economist cites an estimate that fraud is costing the entire healthcare system up to $272 billion. And according to the National Conference of State Legislatures, “fraud and abuse, widespread in both the public and private health care sectors, account for 3 percent to 10 percent of Medicaid payments nationwide.”

The 10 Deadly Sins of Healthcare Fraud

Healthcare fraud, or medical identity fraud as it’s also known, either takes the form of fraudulent billing by unethical providers or misuse of another person’s medical records to obtain care. As the Manor Medical case above illustrates, this kind of fraud may not be discovered for months or years.

Healthcare fraud is an umbrella term covering all manner of unsavory schemes. In 2013, private investigator and consultant Charles Piper, CFE, CRT wrote a revealing article for the Association of Certified Fraud Examiners (ACFE), describing the 10 most popular healthcare provider fraud schemes:
1. Billing for services not rendered. When asking for proof of services, Piper said providers have blamed non-existing floods and fires for missing documents. “I keep waiting for someone to tell me his dog ate the documentation,” he writes.

2. Billing for a non-covered service as a covered service. Piper investigated an allergy doctor who coded an unapproved experimental treatment as something covered by insurance—and got paid for it.

3. Misrepresenting dates of service, such as claiming to treat a patient on two different days instead of one. (More visits, more profits.)

4. Misrepresenting locations of service, such as physicians who billed for services provided in their U.S. offices when they were actually out of the country.

5. Misrepresenting provider of service. A psychological care center hired untrained people to provide therapy. When interviewed, the owner failed to give valid excuses for his crimes, but said that he shouldn’t have to go to jail because he was “extremely overweight.”

6. Waiving of deductibles and/or co-payments, but making up the cost difference by submitting false claims.

7. Incorrect reporting of diagnoses or procedures (includes unbundling). Piper likens unbundling to ordering a five-dollar value meal at a fast-food restaurant, only to find you paid $6.50, because the restaurant charged you for each item in the meal separately.

8. Overutilization of services—billing for unnecessary services. Piper notes alcohol and drug rehabilitation facilities are prime targets for this type of fraud.

9. Corruption (kickbacks and bribery). Fraudsters get quite wily at disguising payments. Piper investigated one provider who paid inflated office rent to another doctor to hide his kickbacks for referring patients.

10. False or unnecessary issuance of prescription drugs. One pharmacist paid for stolen painkillers by making false claims using other people’s identities. When he was caught, the pharmacist told Piper that he needed the painkillers to alleviate the pain from lifting weights. The investigator wryly notes, “(I could tell that he hadn’t been lifting anything heavier than pill bottles.) If he had ingested all the painkillers he stole he would have been dead from an overdose.”

Cracking Down on the Crime of Healthcare Fraud

The Departments of Justice and Health and Human Services have put its collective feet down on healthcare fraud. More than $29.4 billion has been restored to the Medicare Trust Fund since the Health Care Fraud and Abuse Control (HCFAC) Program started in 1997, according to a February 2016 government statement. Compared to the $272-billion problem, that might not seem like a lot, but what is impressive is the government’s return on investment — for every dollar spent in the last three years, the administration recovered $6.10.

Of course, healthcare fraud is not only a government problem—it’s everyone’s problem. Private-public partnerships such as the National Health Care Anti-Fraud Association (NHCAA) and the Medical Identity Fraud Alliance (MIFA) are critical in influencing legislation, providing best practices for fraud prevention and detection, and educating the industry. Patients, too, have the opportunity to be the front line of defense in preventing healthcare fraud and medical identity theft.

As Helen Keller said, “Alone we can do so little, together we can do so much.” Only together can we conquer a crime that affects us all.

SHARE THIS ARTICLE:
Horcruxes in Healthcare: Who Owns Your Medical Identity?

By Doug Pollack, Chief Strategy & Marketing Officer, CIPP/US

In the now-classic Harry Potter series, the villain Voldemort cannot tolerate the idea of death. The most horrific of his many attempts at immortality is when he splits his soul into seven pieces, and “stores” them in powerful objects — so-called Horcruxes. To ensure his survival, Voldemort spreads the Horcruxes far and wide.

Similarly, our personal medical information is scattered far and wide. The recent article, Medical Data Everywhere: Health Revolution or Time Bomb?, identifies just a few healthcare Horcruxes: electronic health records, health information exchanges (HIEs), cloud computing, and a “universe of devices,” including tablet computers, medical implants, and Fitbits.

The Murky Question of Identity Ownership

Arguably, Voldemort “owned” his Horcruxes — they held pieces of his soul, after all. When it comes to our medical identity, the question of ownership is not so clear-cut. The seemingly obvious answer would be us, as patients.

But a fascinating map from healthinfolaw.org reveals that only one out of 50 states — New Hampshire — has a law that says the patient owns the information in his or her medical record. Twenty-one states, including California, Florida, and Texas, give data ownership to hospitals or physicians. The remaining 28 states have no such laws at all.

A Radar.O’Reilly article by Fred Trotter, “Who owns patient data?” suggested that the “notion of ownership is inadequate for health information.” While it seems like it should be an answerable question, he says that “ownership is a poor starting point for health data because the concept itself doesn’t map well to the people and organizations that have relationships with that data.”

The Golden Rule of PHI

Rather than ownership, the more important question is who has what rights to access, modify, append, and share our health records. In other words, how is patient privacy provided for within the digital universe?

One powerful idea is providers as data stewards. As one article in Medical Economics put it, “Experts now counsel physicians against the concept of data ownership entirely. Instead, they encourage physicians
to consider themselves ‘stewards’ of the data within their possession and administrative control.”

Several years ago, the National Committee on Vital and Health Statistics issued a primer on data stewardship. The agency put a biblical spin on its definition: “The fundamental tenet of data stewardship might be expressed as Do unto the data of others as you would have others do unto yours.”

The primer goes on to list four principles and practices of data stewardship:

1. Individual rights, such as a person’s right to access or correct one’s own data
2. The responsibilities of the health data steward, such as ensuring “Data quality, including integrity, accuracy, timeliness, and completeness”
3. Needed security safeguards and controls
4. Accountability, enforcement, and remedies. These include policies for data use and accountability, plus consequences for violation and remediation for affected individuals

We Must Be Good Data Stewards

With a little help from his friends, Harry Potter destroys all of Voldemort’s Horcruxes. But our sensitive medical information lives on in the indestructible Horcruxes of EHRs, the cloud, health information exchanges, and even the Apple watch strapped to our wrists. The individual patient’s ability to control access and use of their data is limited, at best.

Nonetheless, the accelerated pace of cyber attacks on healthcare and other data require patients, healthcare providers, insurers, regulators, and vendors in the private sector to band together to be good stewards of the data that does pass through our hands.

The fundamental tenet of data stewardship might be expressed as Do unto the data of others as you would have others do unto yours.”

— Health Data Stewardship: What, Why, Who, How

Health Data Stewardship

1 http://harrypotter.wikia.com/wiki/Horcrux
2 https://www2.idexpertscorp.com/blog/single/medical-data-everywhere-health-revolution-or-time-bomb
4 http://radar.oreilly.com/2012/06/patient-data-ownership-access.html
6 http://www.ncvhs.hhs.gov/wp-content/uploads/2014/05/090930t.pdf
7 https://www2.idexpertscorp.com/blog/single/the-ever-accelerating-evolution-of-cyber-attacks
About the Authors

Rick Kam
President & Co-Founder

Rick Kam, CIPP/US, is president and co-founder of ID Experts. Kam has extensive experience leading organizations in the development of policies and solutions to address the growing problem of protecting protected health information (PHI) and personally identifiable information (PII), and remediating privacy and security incidents, identity theft, and medical identity theft. Kam leads and participates in several cross-industry data privacy groups, including chair of PHI Protection Network (PPN) and founding member of the Medical Identity Fraud Alliance.

Doug Pollack
CMO ID Experts, CIPP/US

As chief strategy and marketing officer at ID Experts, Doug Pollack is responsible for the strategic direction and marketing of our innovative software and services. He has over 25 years of experience in the technology industry, having held senior management and marketing roles with Apple, Inc., and 3Com Corporation as well as several venture-backed enterprise software startups.

Jeremy Henley
Director of Breach Services

Jeremy Henley is the director of breach services for ID Experts, working hand-in-hand with clients during all steps of breach incident management. With years of sales, consulting and leadership experience, he has also fortified his career in establishing and maintaining relationships with insurance carriers offering cyber and privacy liability coverage and works with insurance brokers and risk managers to minimize the risks of breach. Henley regularly speaks at national conferences on the topics of privacy and security preparedness and data breach response best practices.
Helpful Links & Resources

**Blogs**

Broken Legs & Heart Transplants: Mismatch of Identity Protection Services in Healthcare Data Breach

Over 140,000,000 Americans’ Health Information Disclosed in Data Breaches

Medical Identity Theft: A Deadly Side Effect of Healthcare Data Breaches

5 Ways to Defend Against the Data Breach Epidemic in Healthcare

**Research & Resources**

Study: Sixth Annual Benchmark Study on Privacy and Security of Healthcare Data, Ponemon Institute, May 2016

Breach Response Buyer’s Guide
[www2.idexpertscorp.com/resources/single/breachresponse-buyers-guide/r-general](www2.idexpertscorp.com/resources/single/breachresponse-buyers-guide/r-general)

YourResponse™ Product Datasheet
[https://www2.idexpertscorp.com/resources/single/yourresponse-datasheet/r-general](https://www2.idexpertscorp.com/resources/single/yourresponse-datasheet/r-general)

MyIDCare™ Product Datasheet
[https://www2.idexpertscorp.com/resources/single/myidcare-datasheet/r-general](https://www2.idexpertscorp.com/resources/single/myidcare-datasheet/r-general)

MIDAS™ Product Datasheet

ID Experts’ Blog
[www2.idexpertscorp.com/blog](www2.idexpertscorp.com/blog)

**Products & Services**

Breach Response Services
[https://www2.idexpertscorp.com/data-breach-response](https://www2.idexpertscorp.com/data-breach-response)

MyIDCare™ Identity Protection

Medical Identity Alert System (MIDAS™)
[www2.idexpertscorp.com/midas-software](www2.idexpertscorp.com/midas-software)

ID Experts is a leading provider of identity protection and data breach services for companies and individuals throughout the U.S. We combine consumer-centric software and concierge-style professional services in serving organizations across government, healthcare, commercial enterprises, financial institutions, and higher education.

© Copyright 2017 ID Experts IDE-eBook3 10/17