MegaPath
A Fusion Company

WHITEPAPER

EMPLOYING MANAGED SECURITY SERVICES TO

PREVENT MEDICAL IDENTITY THEFT

MANAGED SECURITY SERVICES

Medical Identity Theft is a Burgeoning Crime

One of the most insidious of identity theft crimes involves stealing another person's medical identity. Medical identity theft is a growing problem in the United States, and according to security research firm The Ponemon Institute, it affected an estimated 1.5 million people last year at a cost of about $30.9B to the industry. The extrapolated per-victim cost is just over $20,000.

A staggering 52% of healthcare organizations surveyed by The Ponemon Institute reported medical identity theft incidents. Alarmingly, the actual number of incidents may be much larger than reported—only about a third of the organizations surveyed felt they had sufficient controls in place to even detect medical identity theft occurrences. Furthermore, it can often take a year or more before victims realize their identities have been compromised, so medical identity theft crimes often go unreported until long after they have occurred.

Why is this crime becoming so prevalent in the United States? There are two driving factors: the increasingly high cost of healthcare and the relatively low risk/high reward nature of medical identity theft crime. To put the value of medical information in perspective, consider this: on the black market, medical identities can go for more than $50 per patient, whereas regular identities are often sold for $1 apiece in quantity.

Why are medical records so valuable, and how are they used?

Medical identities are mainly used to fraudulently obtain prescription drugs, Medicare reimbursement, or medical treatment.

First, let's focus on the top end. Larger scale identity theft schemes usually involve Medicare and prescription fraud, and they are typically orchestrated by organized crime. In fact, this is one of the fastest growing areas of organized crime because it involves substantially less risk than the traditional areas of drugs, prostitution, and gambling.

Some fraud schemes are as simple as recruiting homeless people to visit bogus clinics to get unnecessary treatments that the criminals can then bill to Medicare / Medicaid. On the other hand, there are also very sophisticated operations that will go as far as stealing identities of doctors themselves, setting up fake clinics in their name, and billing and writing prescriptions against stolen patient identities.

Obtaining Fraudulent Services

Although organized crime is a growing problem, the vast majority of medical identity theft crimes are carried out by individuals. Small scale identity theft is usually focused on fraudulently obtaining medical services using someone else's identity. These crimes are often perpetrated by clinical workers, business partners, acquaintances of the victim, or others that have access to records and information. Due to the archaic and fragmented nature of healthcare billing, these individual crimes can go undetected by victims for months or even years.

Medical treatments can be big ticket items, so fraudulent charges of tens of thousands of dollars are not at all uncommon. In one case that was profiled in a Readers Digest article, a pilot from Colorado was billed $41,000 for surgery by a Denver hospital despite the fact that he had never set foot in the hospital. He then had to spend years disputing the charges and nearly filed for bankruptcy because of it.

Losing Your Job, Your Family, or Even Your Life

Beyond pure economic consequences, the results of medical identity theft can be devastating to one's employment, family life, and health.

A woman in Utah was contacted by the state's child protective services unit and told that they were going to take her children away because her newborn baby had tested positive for methamphetamine. This was despite the fact that she did not have a newborn baby, and her youngest child was more than two years old. As it turned out, a pregnant, meth-addicted woman had stolen the other woman's driver license and used it as identification when she checked into a local hospital to give birth.

Even when shown evidence that contradicted their claims of drug abuse and neglect, CPS conducted a full investigation, interviewing the innocent woman's employer, her children, and other people she knew. They eventually dropped the case after a DNA test proved that the woman wasn't the mother of the newborn.

Beyond social and economic consequences, documentation of incorrect medical information in a person's permanent medical record can result in serious injury or death. Imagine if you went to the hospital with a ruptured appendix, but the doctor looked at your record and saw that "you" (aka the person using your medical identity) had your appendix removed a year ago. Appendicitis would likely be ruled out as a cause. Or imagine that you were involved in a car accident and needed a blood transfusion, only the hospital had the blood type of the person who stole your identity instead of your own.

Once incorrect information is added to a file, it's often propagated to other databases and is very difficult to remove. Many medical identity theft victims spend years trying to clean up their records.

Technology Can Be a Problem for Healthcare Organizations

Preventing medical identity theft within an organization is extremely challenging, particularly when new technologies like EMR and wireless systems are introduced. As records become digitized and shared on a network, they become more accessible and easier to transport. A malicious employee can walk off with thousands of records on a flash drive, or a remote attacker can breach an entire database if effective security measures are not in place.

The Healthcare IT Gap

Under the HIPAA security rule, there are administrative, physical and technical safeguard areas. All of these components are vital, but the area that's often the most difficult to deal with is providing adequate technical safeguards.

Healthcare organizations, particularly non-hospital types of organizations, are often under-resourced in their IT departments. The average healthcare organization spends about 2% of its operating budget on IT services versus other industries, like financial services, that spend 10% or more on information technology. This "IT gap" is particularly prevalent in smaller, non-hospital types of healthcare organizations where the compliance burden must be managed with far smaller budgets and fewer employees.

OUTSOURCING AS A SOLUTION

As a healthcare organization, you should protect against losses by putting measures in place to prevent patients using false identities from obtaining services. This can be as simple as checking ID's and training your practitioners to ask background questions to confirm identity.

A more difficult problem is addressing technical safeguards.

The quickest and least expensive way to improve a healthcare organization's security posture is to bring in a managed service provider. There are many advantages to outsourcing security services, including:

- **Reduced long-term hardware and maintenance costs.** When security is offered as a service, the provider owns and manages the equipment, which means that periodic hardware upgrade/replacement is no longer the responsibility of the healthcare organization. Furthermore, maintenance, patching, and break fix are all the responsibility of the provider.
- **CapEx to OpEx.** The avoidance of hardware purchases and associated ongoing upgrades replaces large capital expenditures (CapEx) budget items with predictable monthly operating expenses (OpEx).
- **Scalability.** Managed services are infinitely scalable, so in the case of a merger or acquisition, healthcare organizations can add services rather than re-engineering an entire network.
- **Business continuity and 24-hour service.** Managed service providers generally provide carrier class systems, offering full redundancy, hardened data centers, and around-the-clock monitored security operations centers.
- **Expertise.** You have highly trained security experts at your disposal without hiring expensive staff specialists, which can be a huge benefit particularly if you have a security incident.

IN SUMMARY

- Medical identity theft is a booming segment of fraudulent crime.
- Patients can experience devastating loss as a result of medical identity theft.
- Healthcare technologies like EMR and wireless can increase organizational exposure to medical identity theft crime.
- Many healthcare organizations don't have the resources to effectively implement technical safeguards.
- Managed security services from an outside source can greatly improve security posture and in many cases reduce capital and operational costs.

NEXT STEPS

If patient security concerns are at the forefront for your healthcare organization, consider MegaPath for a fully customizable, dynamic approach designed exclusively with you and your patients in mind.

Go to www.megapath.com/security to learn more about MegaPath Managed Network and Security Services solutions. Or, call MegPath at 877-611-6342 today.