experian health

The Pains of Medical Identity Theft

A look at the trends and how providers can better protect their patients

Contents

Define

What is medical identity theft and why are medical identities targeted?

Medical identity theft occurs when someone steals another person's identity to obtain medical services, treatment, equipment or drugs. It can also occur when criminals use a consumer's personal information to fraudulently bill insurance providers or government programs for medical goods and services never provided.

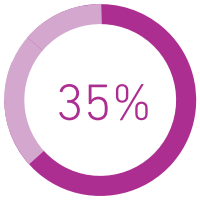
Data from medical identities is **20 to 50 times more valuable** than data from financial sources such as a credit card or Social Security number.

Just think about the wealth of info within a medical identity... social security number, date of birth, address, medical history and health insurance info.

Source: http://www.illuminweb.com/wp-content/uploads/ill-mo-uploads/103/2418/health-systems-cyber-intrusions.pdf

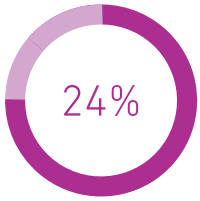
Trends

Medical identity theft has become a major fraud issue over the years.



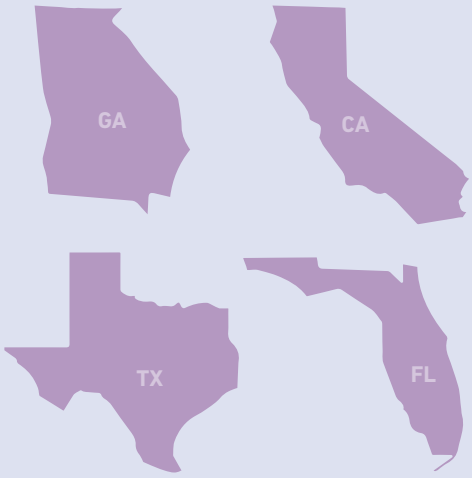
More than **35%** of data breaches in 2019 were medical or healthcare related.
Source: Identity Theft Resource Center

About half of all medical identity theft happens among family members.

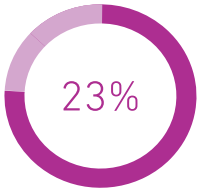


24% of medical identity theft victims said a family member took their medical credentials and used them without permission.

Top States Reporting Medical Identity Theft



Source: https://www.ftc.gov system/files/documents/public_comments/2018/01/00037-142815.pdf



Another **23%** said they willingly shared their healthcare information to help a family member or friend obtain medical care.

Medical ID theft victims spent nearly **$13,500** to resolve their issues, including paying off fraudulent medical bills

Source: Fifth Annual Study on Medical Identity Theft, sponsored by the Medical Identity Fraud Alliance, conducted by the Ponemon Institute

Challenges

Unlike financial fraud, medical identity theft can go undetected for months and co-mingle with a patient's records.

1

People who are victims of medical identity theft may not know about it for weeks, months, or even years. This creates a lag time in reporting because it takes an average of three months to detect.

Source: http://medidfraud.org/wp-content/uploads/2015/02/2014_Medical_ID_Theft_Study1.pdf

2

Most medical identity theft is first detected when a victim gets a collection notice for an unpaid medical bill.

3

If a thief uses a stolen identity to receive treatment, their medical procedures, history, and diagnoses can get mixed up with the victim's own electronic health records—potentially tainting and complicating the victim's care for years to come.

Prescription

Prevention is key as providers can take proactive steps to stop fraud and curb medical identity theft.

Healthcare organizations must commit to a comprehensive digital identity protection strategy to prevent medical identity theft and protect patient privacy.

Extend data security measures beyond the provider organization.

Ensure vendors, as well as patients, are part of the solution to keep sensitive patient information safe. Educate internal staff on security threats and warning signs. Training staff on the types of threats and warnings will help them help you in protecting confidential patient information.

Verify patient identities to protect access to medical record.

The ongoing effort to protect healthcare information requires a multi-layered, multi-solution approach to provide the protection needed in today's risky environment. To avoid HIPAA violations, it is critical to ensure you are giving access to the right patient to view their medical records.

Tip: Asking "out-of-wallet questions" such as a person's city of birth, the name of the patient's high school, or the patient's mother's maiden name can strengthen your patient portal security.

Conclusion

Providers must be proactive, and transparent, taking active steps to confidently authenticate patients and reduce risk during enrollment.

Communicate with patients about the security measures you've invested in, so they understand why they may be asked to verify their information. Patients will feel more secure when they know you've implemented technology that uses a multi-layered approach to determine whether the device has been used to access their account before, as well as whether the device has been used to impersonate other patients in the past.

To learn more about building a robust digital identity protection strategy, visit **www.experianhealth.com/identityproofing**

experian health

06/20 • 1060-EH