CAPLINE
HEALTHCARE MANAGEMENT

Inc. 5000 2018 2019 2020 2022

BBB ACCREDITED BUSINESS A+

MITIGATING MEDICAL IDENTITY THEFT AND FRAUD IN HEALTHCARE

WHAT SHOULD HEALTHCARE PROVIDERS DO?

Google ★★★★★

facebook ★★★★★

www.caplinehealthcaremanagement.com

Overview

Fraud and medical identity theft pose significant challenges to healthcare practices worldwide. These malicious activities involve the fraudulent acquisition and use of personal health information for financial gain, resulting in financial losses, reputational damage, compromised patient care, and regulatory violations for healthcare providers.

Over the years, managing medical fraud and identity theft has become extremely challenging. What is more astonishing is that insurance companies lose several thousand dollars to medical identity theft and fraud every year in the United States.

Healthcare providers are burdened with significant financial losses due to medical identity theft. Fraudulent medical claims, unauthorized procedures, and counterfeit prescriptions can result in substantial monetary damages. The healthcare industry also faces increased operational costs while investigating and rectifying fraudulent activities. These financial repercussions undermine the viability of healthcare systems, diverting resources away from patient care and essential services.

This whitepaper explores the rising concern of fraud and medical identity theft within the healthcare industry and its profound impact on healthcare practices.

Stats Don’t Lie!

Did You Know?

1. More than 10 million citizens become victims of fraud every year in the US, mostly related to stolen identity.

2. Stolen medical data is 20-50 times more valuable than financial data to fraudsters.

3. The largest healthcare data breach in the US happened in 2021, and 3.5 million people were its victims.

4. 1 in 5 medical identity theft victims experiences misdiagnosis and mistreatment.

The Rise of Medical Identity Theft

Medical identity theft has become a pressing concern for healthcare providers. In fact, identity theft complaints related to healthcare in the US accounted for 18% of all identity theft complaints in 2020, states the Federal Trade Commission.

Tech-savvy thieves access information through various digital means. It includes both large-scale criminal hacks to phishing schemes, fraud websites, and sometimes pretending to pose as vendors or IT professionals. This way, a fraudster has immediate access to protected health information (PHI), financial data, and more.

What happens when medical and financial information is compromised?

In medical identity theft, if the data falls into wrong hands, the consequences can extend beyond and the consequences extend beyond mere financial losses, impacting patient safety, provider reputation, and legal implications. It is estimated by the Medical Identity Fraud Alliance that medical identity theft has increased by 113% between 2015 and 2019.

For instance, an individual's personal information is used without consent to obtain medical services and sometimes, the stolen information is also used for submitting false insurance claims. Therefore, it can have devastating financial impacts on the insurer and the insured.

Some of the reasons for medical identity theft includes obtaining prescription drugs to feed an addiction, using credit information to rack up debt, or even blackmailing someone with the threat of posting confidential health information or medical records of public platforms.

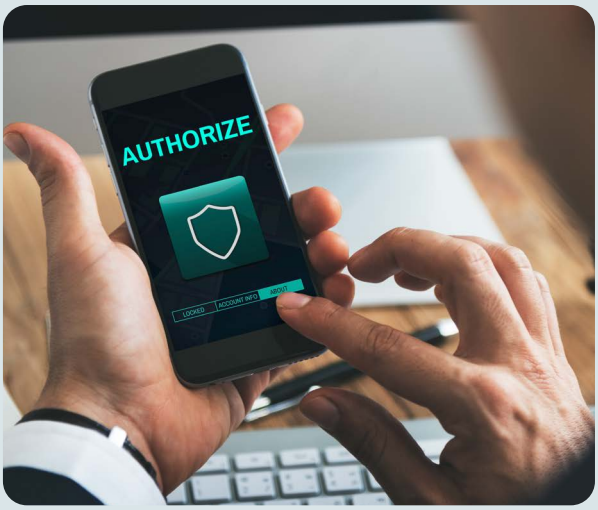
Most Common Types of Medical Identity Theft and Fraud

Scenario 1 - “When Financial Scams Supersede”

Financial fraud involves unauthorized access to a patient's medical records to fraudulently bill for services, medications, or equipment. Perpetrators can submit false claims to insurance companies, leading to financial losses for both patients and healthcare providers.

Scenario 2 - “When Fraudsters Go for Health Insurance Fraud”

In this type of fraud, fraudsters often manipulate insurance information to obtain medical services, prescriptions, or medical equipment. It leads to increased insurance premiums and creates coverage gaps for legitimate policy-holders.



Scenario 3 - “New-age Cybercriminals Breaching Healthcare Data”

Cybercriminals target healthcare databases to steal patient information and then use it for various fraudulent activities. It compromises patient privacy and can have legal and financial implications for healthcare organizations.

How Identity Theft and Fraud Affect Patients and Healthcare Providers

Besides, financial loss, here are some challenges of medical identity theft and fraud

#1 Legal and Regulatory Challenges

It is not a surprise medical identity theft poses legal and regulatory challenges for healthcare providers. The Health Insurance Portability and Accountability Act (HIPAA) in the United States mandates strict data protection and patient privacy standards. Therefore, failure to safeguard patient information can lead to legal consequences, including fines and legal actions. Compliance with these regulations is imperative but often challenging due to the evolving nature of cyber threats and identity theft methods.

#2 Patient Care and Safety Concerns

The impact of medical identity theft also affects patient care and safety. Misattributed medical records can lead to incorrect diagnoses and inappropriate treatments. Moreover, patients may suffer delays in receiving appropriate care as providers work to verify their identities and medical histories. Such disruptions compromise the quality of healthcare and reduce patient trust in the system.

#3 Reputation and Trust

Healthcare providers rely on maintaining a reputation of trust and reliability. Instances of medical identity theft can tarnish their reputation, as patients lose faith in the ability of the provider to secure their confidential information. A breach of patient confidentiality may hamper the bond between healthcare providers and patients. Therefore, causing reputational loss.

How is Capline Helping Providers Address The Issues of Medical Identity Theft and Fraud?

Partnering with Capline Healthcare Management, a trusted HIPAA-compliant organization, for billing, credentialing, and patient eligibility verification services offers significant benefits in mitigating fraud and identity theft in healthcare.

We adhere to stringent security and privacy protocols outlined in the Health Insurance Portability and Accountability Act (HIPAA). These measures are designed to safeguard patients' sensitive health information and personal data.

Your Medical Data Safety Our Commitment!

Choose Capline for

Strong Authentication

For accessing patient records to ensure authorized access only.

Encryption and Security Measures

Robust encryption and security protocols to safeguard patient data.

Regular Auditing of Patient Records

To detect suspicious activities promptly.

Enhanced Patient Verification

Help strengthen patient identity verification processes with two-factor authentication and thorough documentation checks.

Contact Info

thinkgrowth@caplineservices.com

www.caplinehealthcaremanagement.com

888-444-6041

3838 N Sam Houston Pkwy E. Suite 430 Houston, Tx, 77032

Aug 16, 2023