Safeguarding Your Medical Identity

Understanding and Preventing Provider Medical Identity Theft

DEPARTMENT OF HEALTH & HUMAN SERVICES · USA

CMS
CENTERS FOR MEDICARE & MEDICAID SERVICES

Content Summary

Physicians, other providers, and beneficiaries of Medicare and Medicaid are at risk for medical identity theft. The Centers for Medicare & Medicaid Services (CMS) is working to raise awareness among providers to help them protect their medical identities.

This booklet outlines the scope and definition of medical identity theft, common schemes using stolen identities, consequences for victims and perpetrators, mitigation strategies, and appropriate actions for potential victims of medical identity theft. The booklet provides examples of adjudicated criminal cases involving stolen provider medical identities and practical approaches providers can take to protect themselves against medical identity theft.

Proactive approaches include managing enrollment information with payers, monitoring billing and compliance processes, controlling unique medical identifiers, and engaging patients so they are aware of the risks of medical identity theft. No one wants to be a victim of medical identity theft. Providers can use several strategies to protect against it.

Medical Identity Theft Scheme

On February 16, 2012, the ringleader of an illegal prescription drug operation in New York received two consecutive prison sentences totaling 4 to 8 years. In addition to prison, she is required to pay the New York State Medicaid program more than $200,000 for forging more than 250 prescriptions for narcotics. Between 2009 and 2011, she wrote prescriptions using stolen prescription paper obtained from doctors and hospitals in the New York City area. She wrote some of the prescriptions by hand and created others digitally. At the time of her arrest, she had enough paper to write an additional 1,500 prescriptions. Authorities also found a special printer used to process thermal prescriptions. According to law enforcement, "The scope and reach of [her] profit-making operation was significant. As the ringleader, she worked with multiple co-conspirators to create prescriptions in the names of real Medicaid recipients. Working with another group of co-conspirators, she then arranged for the forged prescriptions [using physician medical identifiers] to be filled at pharmacies throughout the state."[1] The theft and misuse of physician and beneficiary medical identifiers was central to this scheme and cost the health care system more than $200,000.

The Scope of Medical Identity Theft

Medical identity theft is a growing and costly issue. Physicians, other providers, and their patients are vulnerable to it. It is defined as "the appropriation or misuse of a patient's or [provider's] unique medical identifying information to obtain or bill public or private payers for fraudulent medical goods or services."[2] This type of theft is one of several forms of health care fraud. The Federal government, in conjunction with State governments, provides health care coverage for more than 100 million people through Medicare, Medicaid, and the Children's Health Insurance Program.[3] That is equivalent to about one out of every three individuals in this country, and expenditures are projected to be more than $1.3 trillion in taxpayer dollars for 2015.[4, 5] The very size of these health care programs makes them targets for fraud. Both the Federal Trade Commission (FTC) and the Centers for Medicare & Medicaid Services (CMS) track cases of provider and patient medical identity theft. The latest FTC data shows that more than 3,900 provider and patient cases of medical identity theft were reported in 2015, with more than 10,000 cases reported between 2013 and 2015.[6]

Common Medical Identity Theft Schemes

All providers are at risk for medical identity theft. Criminals use two major approaches when using stolen medical identities to bill fraudulent claims. In the first approach, provider medical identifiers are used to make it appear as if providers ordered or referred patients for additional health services, such as durable medical

equipment (DME), diagnostic testing, or home health services.[7] For example, on February 9, 2012, the co-owner of a DME company in Texas was sentenced to 99 months in Federal prison for routinely billing Medicaid for medically unnecessary supplies never delivered to beneficiaries. The owner used stolen beneficiary and physician medical identifiers to bill claims to Texas Medicaid; he was ordered to repay nearly $1.5 million to Texas Medicaid in the judgment.[8]

In the second approach, fraudsters use medical identifiers to make it appear that a physician provided and billed services directly. On January 5, 2012, a woman in Florida was sentenced to prison for using a New York physician's medical identifiers from April 2004 through March 2007 to bill for services never rendered. She billed the services to a Medicare Part B carrier in New Jersey. The physician did not know the perpetrator, never saw any of the patients, and did not give permission to use his identity.[9]

Personal and Professional Consequences for Medical Identity Theft Victims

It can take months, sometimes years, to recognize medical identity theft. A provider's first awareness of a stolen medical identity may come in the form of a notice of overpayment from an insurance program demanding immediate repayment or as a notification from the Internal Revenue Service (IRS). For example, if the IRS receives notification that a provider of record has earned income for services rendered when those services were never reported on required tax documents, the IRS may send that provider a demand for payment. Responding to overpayment demand letters, responding to IRS notification letters, and correcting credit issues that can arise from medical identity theft are among the many potential consequences a provider may face. Financial problems associated with medical identity theft can be a major problem for a provider. Sorting out the problems can require a lot of time, effort, and money. It may be necessary to hire an attorney to correct the financial problems.

Other potential medical identity theft problems with difficult consequences for a provider can include the impact on a provider's practice and reputation. A provider could lose business if patients or other providers are aware of an investigation. Quality reporting data can be skewed if false data is added to a provider's legitimate data. Being the provider of record for billed services the provider never furnished

can create the financial problems already mentioned, as well as calls, questions, and complaints from other providers and patients reviewing bills with services charged in the provider's name.

Legal Consequences for Medical Identity Thieves

In December 2015, the Patient Access and Medicare Protection Act became law. Section 8 of the law amended section 1128B(b) of the Social Security Act to stiffen penalties for provider and beneficiary identity theft. If anyone without proper authority "knowingly and willfully purchases, sells or distributes, or arranges for the purchase, sale, or distribution" of any provider or beneficiary identification number under Medicare, Medicaid, or Children's Health Insurance Programs, the maximum penalties are 10 years in prison, a $500,000 fine for individuals or $1,000,000 for corporations, or both. Of course, other criminal and civil statutes will apply if the misappropriated identifiers are used to submit fraudulent claims.[10]

Allowing the Misuse of Medical Identifiers Poses a Significant Risk

The consequences of medical identity theft for providers can be severe even when they have done nothing wrong. Most providers are honest and do the right thing. In some cases, providers voluntarily permit or promote the misuse of their identities for a variety of reasons, which places them at significant risk for theft. Purposeful misuse of identifiers can also lead to consequences such as civil monetary penalties,[11] criminal fines and restitution,[12] prison time,[13] and exclusion from Medicare and Medicaid.[14]

Common examples of ways providers allow the misuse of their medical identifiers include:

- Signing referrals for patients they do not know;
- Signing Certificates of Medical Necessity (CMNs) for patients they know but who do not need the service or supplies;
- Signing CMNs even though their own documentation disputes medical need;
- Signing CMNs for more services than what are medically necessary; and
- Signing blank referral forms.[15]

Some people who want to abuse the system try to make a case that, out of sympathy or convenience, the provider should accommodate one or more of these requests. But since the provider's signature is intended to authorize the services provided, the provider is ultimately liable for false or fraudulent claims with their authentic signature, even without evidence of other fraud.[16]

As one example shows, on January 12, 2012, a physician was sentenced to prison for committing health care fraud. This physician accepted co-ownership of a health care clinic opened by a fraudster who was recruiting doctors. The physician never treated any of the patients but allowed the submission of claims in his name. He received patient files transported to his office, at a separate location, where he signed off on the services.[17] Another defendant was later sentenced to more than 3 years in prison and ordered to pay more than $600,000 in restitution.[18]

Mitigate Risks

Providers are responsible for their medical identifiers to the extent they can protect them and mitigate their vulnerability to theft. Four strategies providers can use to protect themselves and their practices include actively managing enrollment information with payers, monitoring billing and compliance processes, controlling unique medical identifiers, and engaging patients in a conversation about medical identity theft.

Actively Manage Enrollment Information with Payers

You can actively manage enrollment information with payers by updating them about material enrollment changes, especially when opening, closing, or moving practice locations or when separating from an organization. You should always keep your reimbursement banking information current so payers can alert you to problems, such as additional billings from old locations or new locations opened without the provider's knowledge.

Monitor Billing and Compliance Processes

You can strengthen compliance activities by implementing sound policies and procedures to minimize your risk and improve overall program integrity. The U.S. Department of Health and Human Services, Office of Inspector General (HHS-OIG) has developed guidelines providers can use to improve business practices.[19] While not required of all providers, the guidelines are comprehensive and helpful. Visit https://oig.hhs.gov/compliance/compliance-guidance/index.asp website to review compliance guidelines.

Adopting sound billing practices is an extremely important strategy and cannot be overemphasized. You should be aware of billings in your name, paying close

attention to the organization(s) to which you have assigned billing privileges. Actively review organizational remittance notices, and compare them with medical record documentation. Monitor mid-level provider activities and charting to ensure that documentation supports billed services. Read all documents before you sign them and keep copies. Document any conversation(s) you have with someone else about billing issues, and report suspected fraud.

Remember, whether staff or a third-party biller completes the claims processing services, the provider of record is responsible for the billings submitted. A provider's signature certifies the truth and accuracy of signed and submitted claims.[20] Ensure all services billed are accurate and supported in the medical record.

Control Unique Medical Identifiers

Prospective Employers: Providers should avoid giving identifiers to potential employers or organizations before taking the time to learn about them. Check out prospective employers before applying to work with them or handing over medical identifying information.

Train Staff: Providers should train their staff on the appropriate use and distribution of medical identifiers, including when not to distribute them. For example, they should train staff to question unknown providers who contact the office. If office policy allows information sharing over the phone, staff should take a caller's telephone number and call them back with the information so they can authenticate the call. Another precaution staff should take is to compare where a referring provider is located in relation to the office and the patient's residence. If the distance seems unreasonable, additional calls may be required.[21] Providers should carefully consider which staff will have access to their medical identifiers.

Control Prescription Pads: Medicaid regulations require use of tamper-resistant prescription pads. All written prescriptions must include at least one security feature from each of the following categories:

- One or more industry-recognized features designed to prevent unauthorized copying of a completed or blank prescription form;
- One or more industry-recognized features designed to prevent the erasure or modification of information written on the prescription pad by the prescriber; and
- One or more industry-recognized features designed to prevent the use of counterfeit prescription forms.[22]

Additional precautions are reasonable. For example, providers should not inadvertently leave prescription pads unattended in examination rooms or other

public areas. Prescription pads should be locked up when not in use, and not left visible in the provider's car. Providers should take a daily count of prescription pads and clearly and completely fill out prescriptions and other documents to prevent tampering.

Engage Patients

As a provider, you are in an excellent position to raise awareness with patients about medical identity theft and the problems and dangers associated with it. While most patients automatically receive medical bills and an explanation of benefits (EOBs) following an appointment, Medicaid patients normally do not. Providers should encourage patients to request and review their medical bills. By reviewing bills, patients may be able to spot medical identity theft by identifying services they did not receive. Providers should also encourage patients to review their EOBs, including their Medicare Summary Notices and Medicaid bills.

Remediation for Victims

Assistance is available for victims of medical identity theft. The CMS Center for Program Integrity is working hard to assist victims through a validation/remediation initiative. The goal of the process is to respond to legitimate provider needs, to establish a consistent process for determining and validating provider victims of identity theft, and to help absolve the financial problems related to the theft, such as Medicare overpayments or tax obligations. For a description of the remediation process and whom to contact if you experience problems, visit https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/MedicareProviderSupEnroll/downloads//ProviderVictimPOCs.pdf on the CMS website. In addition to this remediation process—through additional tools, such as predictive modeling and rigorous screening for enrollees, and through preventive policies, such as suspending payments to suspected criminals[23]—CMS is working to eliminate medical identity theft.

Report It

Any provider concerned that they may be the victim of medical identity theft should contact:

- Local law enforcement service in your area
- State Medicaid agency:

  Website: https://oig.hhs.gov/fraud/medicaid-fraud-control-units-mfcu/files/contact-directors.pdf (click the State where you practice for the appropriate contact information, and then notify the agency)

- FTC Identity Theft Hotline to report misuse of your personal information:

  Phone: 1-877-438-4338 (1-877-ID-THEFT)
  TTY: 1-866-653-4261
  Website: https://www.consumer.ftc.gov/features/feature-0014-identity-theft

- HHS-OIG hotline to report suspected fraud:

  Phone: 1-800-447-8477 (1-800-HHS-TIPS)
  TTY: 1-800-377-4950
  Fax: 1-800-223-8164
  Email: HHSTips@oig.hhs.gov
  Website: https://oig.hhs.gov/fraud/report-fraud

- U.S. Department of Health and Human Services regional office:

  Website: http://www.hhs.gov/about/agencies/regional-offices (click your region for contact information)

To see the electronic version of this booklet and the other products included in the "Safeguarding Your Medical Identity" Toolkit, visit the Medicaid Program Integrity Education page at https://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/Medicaid-Integrity-Education/edmic-landing.html on the CMS website.

Follow us on Twitter #MedicaidIntegrity

References

1 New York Office of the Attorney General. (2012, February 16). As Rx Abuse Rises, A.G. Schneiderman Announces Prison Sentence for Woman Who Forged More Than 250 Painkiller Prescriptions. Retrieved March 7, 2016, from http://www.ag.ny.gov/press-release/rx-abuse-rises-ag-schneiderman-announces-prison-sentence-woman-who-forged-more-250

2 Agrawal S. & Budetti P. (2012, February 1). Physician Medical Identity Theft. The Journal of the American Medical Association, 307(5), 459–460. Retrieved March 7, 2016, from http://jama.jamanetwork.com/article.aspx?articleid=1104942

3 Centers for Medicare & Medicaid Services. CMS Covers 100 Million People. Retrieved March 7, 2016, from http://www.cms.gov/

4 Kaiser Family Foundation. State Health Facts. Health Insurance Coverage of the Total Population. Retrieved March 7, 2016, from http://kff.org/other/state-indicator/total-population/

5 Centers for Medicare & Medicaid Services. (2015, July 30). National Health Expenditure Data: Projected. NHE Projections 2014–2024—Tables. Table 3: National Health Expenditures; Aggregate and per Capita Amounts, Percent Distribution and Annual Percent Change by Source of Funds: Calendar Years 2008–2024. Retrieved March 7, 2016, from https://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/NationalHealthAccountsProjected.html

6 Federal Trade Commission. (2016, February). Consumer Sentinel Network Data Book for January–December 2015. Retrieved March 7, 2016, from https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2015/160229csn-2015databook.pdf

7 Agrawal S. & Budetti P. (2012, February 1). Physician Medical Identity Theft. The Journal of the American Medical Association, 307(5), 459–460. Retrieved March 7, 2016, from http://jama.jamanetwork.com/article.aspx?articleid=1104942

8 U.S. Attorney's Office. Southern District of Texas. (2012, February 9). Former DME Company Owner Lands in Federal Prison. Retrieved March 7, 2016, from https://www.justice.gov/archive/usao/txs/1News/Releases/2012%20February/120209%20Essien.html

9 U.S. Attorney's Office. Middle District of Florida. (2012, January 5). Sarasota County Woman Sentenced for Health Care Fraud. Retrieved March 7, 2016, from https://www.fbi.gov/tampa/press-releases/2012/sarasota-county-woman-sentenced-for-health-care-fraud/

10 U.S. Congress. (2015, December 28). Patient Access and Medicare Protection Act. Retrieved March 9, 2016, from https://www.congress.gov/bill/114th-congress/senate-bill/2425/text?q=%7B%22search%22%3A%5B%22medicare+identity+theft%22%5D%7D&resultIndex=2

11 Social Security Act § 1128A(a)(1), (3). Civil Monetary Penalties. Retrieved March 7, 2016, from https://www.ssa.gov/OP_Home/ssact/title11/1128A.htm

12 False Claims, 31 U.S.C. § 3729(a) and (b). Retrieved March 7, 2016, from https://www.gpo.gov/fdsys/pkg/USCODE-2013-title31/html/USCODE-2013-title31-subtitleIII-chap37-subchapIII-sec3729.htm

13 False, Fictitious, or Fraudulent Claims, 18 U.S.C. § 287. Retrieved March 7, 2016, from https://www.gpo.gov/fdsys/pkg/USCODE-2013-title18/html/USCODE-2013-title18-partI-chap15-sec287.htm

14 Social Security Act § 1128(b)(6)(B). Exclusion of Certain Individuals and Entities From Participation in Medicare and State Health Care Programs. Retrieved March 7, 2016, from https://www.ssa.gov/OP_Home/ssact/title11/1128.htm

15 Medicare Learning Network. (2014, October). Medicaid Program Integrity: Understanding Provider Medical Identity Theft. Retrieved March 7, 2016, from https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/Med-ID-Theft-Booklet-ICN908264.pdf

16 Medicare Learning Network. (2014, October). Medicaid Program Integrity: Understanding Provider Medical Identity Theft. Retrieved March 7, 2016, from https://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/Med-ID-Theft-Booklet-ICN908264.pdf

17 U.S. Department of Justice. Federal Bureau of Investigation. (2012, January 12). Physician Sentenced to Eight Years in Federal Prison for Role in Massive Medicare Fraud Scam. Retrieved March 7, 2016, from https://www.fbi.gov/sacramento/press-releases/2012/physician-sentenced-to-eight-years-in-federal-prison-for-role-in-massive-medicare-fraud-scam

18 U.S. Department of Justice. Eastern District of California. (2014, January 9). Southern California Doctor Sentenced to Over 3 Years in Prison for Medicare Fraud Scheme. Retrieved March 7, 2016, from https://www.justice.gov/usao-edca/pr/southern-california-doctor-sentenced-over-3-years-prison-medicare-fraud-scheme

19 U.S. Department of Health and Human Services. Office of Inspector General. Compliance Guidance. Retrieved March 7, 2016, from https://oig.hhs.gov/compliance/compliance-guidance/index.asp

20 U.S. Department of Health and Human Services. Office of Inspector General. (2000, October 5). Notices. 65 Fed. Reg. 59434–59435. Retrieved March 7, 2016, from https://www.gpo.gov/fdsys/pkg/FR-2000-10-05/pdf/00-25500.pdf

21 U.S. Department of Health and Human Services. Office of Inspector General. (2012, March 13). Office of Investigations Representative.

22 U.S. Department of Health and Human Services. Center for Medicare & Medicaid Services. Center for Medicaid and State Operations. (2007, August 17). State Medicaid Director Letter #07-012. Retrieved March 7, 2016, from https://downloads.cms.gov/cmsgov/archived-downloads/SMDL/downloads/SMD081707.pdf

23 U.S. Department of Health and Human Services. (2011, February 2). Rules and Regulations. 76 Fed. Reg. 5862. Retrieved March 7, 2016, from https://www.gpo.gov/fdsys/pkg/FR-2011-02-02/pdf/2011-1686.pdf

Disclaimer

This booklet was current at the time it was published or uploaded onto the web. Medicaid and Medicare policies change frequently so links to the source documents have been provided within the document for your reference.

This booklet was prepared as a service to the public and is not intended to grant rights or impose obligations. This booklet may contain references or links to statutes, regulations, or other policy materials. The information provided is only intended to be a general summary. Use of this material is voluntary. Inclusion of a link does not constitute CMS endorsement of the material. We encourage readers to review the specific statutes, regulations, and other interpretive materials for a full and accurate statement of their contents.

April 2016