

Partners in Integrity

Understanding and Preventing Provider Medical Identity Theft



Content Summary

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, 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 pragmatic approaches they can use 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 consecutive prison sentences totaling between 4 and 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 over 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 amounts to expenditures of more than \$836 billion in taxpayer dollars per year.[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 3,300 physician and patient cases of medical identity theft were reported in 2014, with more than 8,000 cases reported between 2012 and 2014.[6]

Common Medical Identity Theft Schemes

All providers are at risk for medical identity theft. Criminals use two major approaches to bill fraudulent claims with stolen medical identities. 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 totaling more than \$2 million.[8] In the second approach, fraudsters use provider 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]

Consequences of Medical Identity Theft

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 the problems out can require a lot of time, effort, and money. An attorney may be required to assist in correcting the financial problems incurred.

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.

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,[10] criminal fines and restitution,[11] prison time,[12] and exclusion from Medicare and Medicaid.[13]

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 than what patients actually need; and
- Signing blank referral forms.[14]

Patients, other providers, or “fraudsters may ask [a provider] to accommodate these types of requests. It is important that [all providers] understand [they can] be held liable for these actions”[15] even without evidence of other fraud.

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 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.[16]

Mitigate Risks

You are responsible for your medical identifiers to the extent you can protect them and mitigate your 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. By keeping information current, payers can alert providers 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.[17] While not required of all providers, the guidelines are comprehensive and helpful. Visit <https://oig.hhs.gov/compliance/compliance-guidance/index.asp> on the HHS-OIG 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 reassigned 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.[18] Ensure all services billed are accurate and supported in the medical record.

CONTROL UNIQUE MEDICAL IDENTIFIERS

Prospective Employers: Avoid giving your 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: Train your staff on the appropriate use and distribution of your medical identifiers, including when not to distribute them. For example, make sure to train staff to question unknown providers who contact your office. If office policy allows information sharing over the phone, require staff to take a caller's telephone number and call them back with the information so staff can authenticate the call. Another precaution staff can take is to compare the location of a referring provider in relation to the office and the patient's residence. If the distance seems unreasonable, additional calls may be required.[19] Carefully consider which staff will have access to your medical identifiers.

Control Prescription Pads: Medicaid regulations require use of tamper-resistant prescription pads. All written prescriptions must include security features like a watermark or thermal ink, which shows any attempt to alter a prescription, and industry-recognized design features that prevent counterfeit prescriptions.[20] Additional precautions are reasonable. For example, do not inadvertently leave prescription pads unattended in examination rooms or other public areas. Keep prescription pads locked up when not in use, and do not leave them visible in your car. You may want to take a daily count of prescription pads. Also, 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. Encourage patients to request and review their medical bills. By reviewing bills, they may be able to spot medical identity theft by identifying services they did not receive. 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 (CPI) 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 who 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,[21] CMS is working to eliminate medical identity theft.

Report It

Any provider concerned that he or she may be the victim of medical identity theft should contact:

- Local law enforcement service in your area
- State Medicaid agency—Visit <https://oig.hhs.gov/fraud/medicaid-fraud-control-units-mfcu/files/contact-directors.pdf> on the HHS-OIG website. Click on the State where you practice for the appropriate contact information, and then notify the agency.
- Federal Trade Commission (FTC)—Contact the FTC’s Identity Theft Hotline to report misuse of your personal information:
Phone: 1-877-438-4338 (1-877-ID-THEFT)
TTY: 1-800-377-4950
Website: <http://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://forms.oig.hhs.gov/hotlineoperations/>
- Health and Human Services regional office—Visit <http://www.hhs.gov/iea/regional/index.html> on the U.S. Department of Health and Human Services website, and click on your region for contact information.

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

Follow us on Twitter  [#MedicaidIntegrity](https://twitter.com/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 June 8, 2015, 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 June 8, 2015, from <http://jama.jamanetwork.com/issue.aspx?issueid=22488>
- 3 Centers for Medicare & Medicaid Services. CMS Covers 100 Million People... Retrieved June 8, 2015, from <http://www.cms.gov/>
- 4 Kaiser Family Foundation. State Health Facts. Health Insurance Coverage of the Total Population. Retrieved April 6, 2015, from <http://kff.org/other/state-indicator/total-population/>
- 5 Center on Budget and Policy Priorities. (2015, March 11). Policy Basics: Where Do Our Federal Tax Dollars Go? Retrieved April 7, 2015, from <http://www.cbpp.org/cms/?fa=view&id=1258>
- 6 Federal Trade Commission. (2015, February). Consumer Sentinel Network Data Book for January–December 2014. Retrieved April 6, 2015, from <https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december-2014/sentinel-cy2014-1.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 June 8, 2015, from <http://jama.jamanetwork.com/issue.aspx?issueid=22488>
- 8 U.S. Attorney’s Office. Southern District of Texas. (2012, February 9). Former DME Company Owner Lands in Federal Prison. Retrieved June 8, 2015, from <http://www.fbi.gov/houston/press-releases/2012/former-dme-company-owner-lands-in-federal-prison>
- 9 U.S. Attorney’s Office. Middle District of Florida. (2012, January 5). Sarasota County Woman Sentenced for Health Care Fraud. Retrieved June 8, 2015, from <http://www.fbi.gov/tampa/press-releases/2012/sarasota-county-woman-sentenced-for-health-care-fraud/>
- 10 Social Security Act § 1128A(a)(1),(3). Civil Monetary Penalties. Retrieved June 8, 2015, from http://www.ssa.gov/OP_Home/ssact/title11/1128A.htm
- 11 False Claims, 31 U.S.C. § 3729(a) and (b). Retrieved April 7, 2015, from <http://www.gpo.gov/fdsys/pkg/USCODE-2013-title31/html/USCODE-2013-title31-subtitleIII-chap37-subchapIII-sec3729.htm>
- 12 False, Fictitious, or Fraudulent Claims, 18 U.S.C. § 287. Retrieved April 7, 2015, from <http://www.gpo.gov/fdsys/pkg/USCODE-2013-title18/html/USCODE-2013-title18-partI-chap15-sec287.htm>
- 13 Social Security Act § 1128(b)(6)(B). Exclusion of Certain Individuals and Entities From Participation in Medicare and State Health Care Programs. Retrieved June 8, 2015, from http://www.ssa.gov/OP_Home/ssact/title11/1128.htm
- 14 Medicare Learning Network. (2014, October). Medicaid Program Integrity: Understanding Provider Medical Identity Theft. Retrieved April 15, 2015, from <http://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/Med-ID-Theft-Booklet-ICN908264.pdf>
- 15 Medicare Learning Network. (2014, October). Medicaid Program Integrity: Understanding Provider Medical Identity Theft. Retrieved April 15, 2015, from <http://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/Med-ID-Theft-Booklet-ICN908264.pdf>
- 16 U.S. Department of Justice. (2012, January 12). Physician Sentenced to Eight Years in Federal Prison for Role in Massive Medicare Fraud Scam. Retrieved June 8, 2015, from <http://www.fbi.gov/sacramento/press-releases/2012/physician-sentenced-to-eight-years-in-federal-prison-for-role-in-massive-medicare-fraud-scam>
- 17 U.S. Department of Health and Human Services. Office of Inspector General. Compliance Guidance. Retrieved June 8, 2015, from <https://oig.hhs.gov/compliance/compliance-guidance/index.asp>

18 U.S. Department of Health and Human Services. Office of Inspector General. (2000, October 5). Notices. 65 Fed. Reg. 59434–59435. Retrieved June 8, 2015, from <http://www.gpo.gov/fdsys/pkg/FR-2000-10-05/pdf/00-25500.pdf>

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

20 Medicare Learning Network. (2014, October). Medicaid Program Integrity: Understanding Provider Medical Identity Theft (p. 4). Retrieved April 13, 2015, from <http://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/Med-ID-Theft-Booklet-ICN908264.pdf>

21 U.S. Department of Health and Human Services. (2011, February 2). Rules and Regulations. 76 Fed. Reg. 5862. Retrieved June 8, 2015, from <http://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.

June 2015



June 2015