DEPARTMENT OF HEALTH AND HUMAN SERVICES
Centers for Medicare & Medicaid Services

Medicare Learning Network®
Official Information Health Care Professionals Can Trust

Medicaid Program Integrity:

Understanding and Preventing Provider Medical Identity Theft

ICN 908264 October 2014

DISCLAIMERS

This booklet was current at the time it was published or uploaded onto the web. Medicare/Medicaid policy changes 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. It is not intended to take the place of either the written law or regulations. We encourage readers to review the specific statutes, regulations, and other interpretive materials for a full and accurate statement of their contents.

The Medicare Learning Network® (MLN), a registered trademark of CMS, is the brand name for official information health care professionals can trust. For additional information, visit the MLN's web page at http://go.cms.gov/MLNGenInfo on the CMS website.

Your feedback is important to us and we use your suggestions to help us improve our educational products, services and activities and to develop products, services and activities that better meet your educational needs. To evaluate Medicare Learning Network® (MLN) products, services and activities that you have participated in, received, or downloaded, please go to http://go.cms.gov/MLNProducts and in the left-hand menu click on the link called 'MLN Opinion Page' and follow the instructions. Please send your suggestions related to MLN product topics or formats to MLN@cms.hhs.gov.

Table of Contents

Please note: The information in this publication only applies to Medicaid programs. However, you may find the information useful even if you do not participate in Medicaid.

Overview

Physicians and other providers of Medicaid services are at risk for medical identity theft. The Centers for Medicare & Medicaid Services (CMS) works to raise awareness among all 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 you can use to protect yourself 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. You can use several strategies to protect yourself 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 must 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. Law enforcement also found a special printer used to process thermal prescriptions. Working with multiple co-conspirators, she used real names of Medicaid recipients on the prescriptions, and then filled the prescriptions in pharmacies across New York. The theft and misuse of physician and beneficiary medical identifiers, central to this scheme, cost the health care system more than $200,000.

The Scope of Medical Identity Theft

Medical identity theft 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," according to S. Agrawal and P. Budetti in their article, "Physician Medical Identity Theft," in the "Journal of the American Medical Association." It is a growing and costly issue. You, other providers, and patients are vulnerable to it. 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 100 million people through Medicare, Medicaid, and the Children's Health Insurance Program (CHIP) (1), which is equivalent to about one out of every four individuals in this country, and amounts to expenditures of more than $732 billion in taxpayer dollars per year (2). The size of these health care programs makes them targets for fraud. Both the Federal Trade Commission (FTC) and CMS track cases of provider and patient medical identity theft. The latest FTC data shows that more than 3,600 physician and patient cases of medical identity theft were reported in 2009, with more than 12,000 cases reported between 2007 and 2009 (3).

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, criminals use provider medical identifiers 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. 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.

In the second approach, criminals 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 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.

Consequences of Medical Identity Theft

It can take months, sometimes years, before someone recognizes medical identity theft. You may first become aware of a stolen medical identity when you receive 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 earned income for services rendered when those services were never reported on required tax documents, that provider may receive tax forms for income never received with a demand for payment.

You may face many potential consequences, including responding to overpayment demand letters, responding to IRS notification letters, and correcting credit issues that can arise from medical identity theft. Financial problems associated with medical identity theft can present a major problem for you. Sorting the problems out can require a lot of time, effort, and money. You may need an attorney to assist in correcting the financial problems incurred.

Other potential medical identity theft problems with difficult consequences for you include the impact on your practice and reputation. Your utilization may suffer if patients or other providers become aware of an investigation. False data added to your legitimate data can skew quality reporting data. Being the provider of record for billed services you 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 your name. Most importantly, all of these problems may negatively affect your reputation.

Allowing the Misuse of Medical Identifiers Poses a Significant Risk

The consequences of medical identity theft can be severe, even when you did 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 – this places them at significant risk for subsequent theft. Purposeful misuse of identifiers can also lead to consequences such as civil monetary penalties, criminal fines and restitution, prison time, and exclusion from Medicare and Medicaid. Common examples of ways providers allow the misuse of their medical identifiers include signing:

- Blank referral forms;
- Certificates of Medical Necessity (CMNs) for patients they know but who do not need the service or supplies;
- CMNs even though their own documentation disputes medical need;
- CMNs for more than what patients actually need; and
- Referrals for patients they do not know.

Patients, other providers, or fraudsters may ask you to accommodate these types of requests. It is important that you understand you may be liable for these actions.

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.

Mitigating Risks

You are responsible for your medical identifiers to the extent you can protect them and mitigate your vulnerability to theft. Four strategies you can use to protect yourself and your practice include:

1. Actively managing enrollment information with payers;
2. Controlling unique medical identifiers;
3. Engaging patients in a conversation about medical identity theft; and
4. Monitoring billing and compliance processes.

Actively Manage Enrollment Information with Payers

You can actively manage enrollment information with payers by updating them about material enrollment changes, especially when:

- Changing banking information;
- Opening, closing, or moving practice locations; or
- Separating from an organization.

You should always keep your reimbursement banking information current. By keeping information current, payers can alert you to problems, such as additional billings from old locations or new locations opened without your knowledge.

Control Unique Medical Identifiers

Prospective Employers: Avoid giving your identifiers to potential employers or organizations before taking the time to learn about them. Investigate 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. Compare the location of a referring provider in relation to the office and the patient's residence. If the distance seems unreasonable, make additional calls. Carefully consider which staff may access your medical identifiers.

Control Prescription Pads: Medicaid regulations began requiring tamper-resistant prescription pads on April 1, 2008. All written prescriptions must include security features like a watermark or thermal ink that shows any attempt to alter a prescription, and industry-recognized design features that prevent counterfeit prescriptions. Take additional reasonable precautions. 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 in a Conversation About Medical Identity Theft

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 (EOB) following an appointment, Medicaid patients normally do not. Encourage patients to request and review their medical bills. By reviewing bills, they may 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.

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 & Human Services (HHS), Office of Inspector General (OIG) developed guidelines you can use to improve business practices. While not required of all providers, the guidelines are comprehensive and helpful. For more information on compliance guidelines, visit https://oig.hhs.gov/compliance/compliance-guidance on the OIG website.

Adopting sound billing practices is an extremely important strategy and cannot be overemphasized. Keep aware of billings in your name and pay close attention to the organizations to which you reassigned billing privileges. This includes:

- Actively reviewing organizational remittance notices and comparing them with medical record documentation;
- Documenting any conversations with someone else about billing issues;
- Monitoring mid-level provider activities and charting them to ensure that documentation supports billed services;
- Reading all documents before you sign them and keeping copies; and
- Reporting suspected fraud.

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

Remediation for Victims

Assistance is available for victims of medical identity theft. The CMS Center for Program Integrity (CPI) works hard to assist victims through a validation/remediation initiative. The initiative's goals include responding to legitimate provider needs, establishing a consistent process for determining and validating provider victims of identity theft, and helping 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, refer to http://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/MedicareProviderSupEnroll/Downloads/ProviderVictimPOCs.pdf on the CMS website.

In addition to this remediation process, CMS continues to work on eliminating medical identity theft through additional tools and preventive policies, such as predictive modeling, rigorous screening for enrollees, and suspending payments to suspected criminals.

Report It

If you think that you may be the victim of medical identity theft, contact:

- **Your Local Law Enforcement**
- **Your State Medicaid Agency**

  http://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/FraudAbuseforProfs
- **Federal Trade Commission (FTC) Identity Theft Hotline**

  Phone: 1-877-438-4338 (1-877-ID-THEFT)

  TTY: 1-866-653-4261

  Website: http://www.consumer.ftc.gov/features/feature-0014-identity-theft
- **HHS OIG Hotline**

  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
- **Your Regional HHS Office**

  http://www.hhs.gov/about/foa/regions

  Click on your region for the appropriate contact information, and then notify the regional office.

Resources

- For additional information and educational materials related to provider compliance, visit http://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/ProviderCompliance.html on the CMS website, or scan the Quick Response (QR) code on the right with your mobile device.

- To download additional Medicare Learning Network® (MLN) products designed to educate Medicare and Medicaid providers about medical identity, refer to http://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/Downloads/SafeMed-ID-Products.pdf on the CMS website. These products include a web-based training course titled "Safeguarding Your Medical Identity," which is approved for Continuing Education (CE) credit. Please note, you **must** register and complete a post-assessment test and evaluation to receive Continuing Education Units (CEUs) or Continuing Medical Education (CME) credit for this course. To register for this course, go to the MLN Web-Based Training (WBT) web page at http://www.cms.gov/Outreach-and-Education/Medicare-Learning-Network-MLN/MLNProducts/WebBasedTraining.html on the CMS website.

The following resources were used to compile the information in this booklet:

- "As Rx Abuse Rises, A.G. Schneiderman Announces Prison Sentence For Woman Who Forged More Than 250 Painkiller Prescriptions," press release by the New York State Attorney General (February 16, 2012) http://www.ag.ny.gov/press-release/rx-abuse-rises-ag-schneiderman-announces-prison-sentence-woman-who-forged-more-250
- Civil Monetary Penalties – Social Security Act, Sections 1128A(a)(1) and (3) http://www.ssa.gov/OP_Home/ssact/title11/1128A.htm
- "CMS Initiative to Help Victims of Provider Medical Identity Theft" by T. Doolittle, 2011 Public Comments (Retrieved March 3, 2012)
- CMS website http://www.cms.gov
- "Consumer Sentinel Network Data Book for January–December 2009" (February 2010) http://www.ftc.gov/sites/default/files/documents/reports_annual/sentinel-cy-2009/sentinel-cy2009.pdf
- Exclusion of Certain Individuals and Entities from Participation in Medicare and State Health Care Programs – Social Security Act, Section 1128(b)(6)(B) http://www.socialsecurity.gov/OP_Home/ssact/title11/1128.htm
- False Claims – Liability for Certain Acts, Definitions – 31 United States Code (U.S.C.) Sections 3729(a) and (b) http://www.gpo.gov/fdsys/pkg/USCODE-2013-title31/pdf/USCODE-2013-title31-subtitleIII-chap37-subchapIII-sec3729.pdf
- False, Fictitious or Fraudulent Claims – 18 U.S.C. Section 287 http://www.gpo.gov/fdsys/pkg/USCODE-2013-title18/pdf/USCODE-2013-title18-partI-chap15-sec287.pdf
- "Former DME Company Owner Lands in Federal Prison," press release by the U.S. Attorney's Office, Southern District of Texas (February 9, 2012) http://www.justice.gov/usao/txs/1News/Releases/2012%20February/120209%20Essien.html

- "Medicare, Medicaid, and Children's Health Insurance Programs; Additional Screening Requirements, Application Fees, Temporary Enrollment Moratoria, Payment Suspensions and Compliance Plans for Providers and Suppliers," Final Rule, 76 Federal Register 5862 (February 2, 2011) http://www.gpo.gov/fdsys/pkg/FR-2011-02-02/pdf/2011-1686.pdf
- OIG Compliance Guidance https://oig.hhs.gov/compliance/compliance-guidance
- "OIG Compliance Program for Individual and Small Group Physician Practices," Notice, 65 Federal Register 59434 – 59435 (October 5, 2000) http://www.gpo.gov/fdsys/pkg/FR-2000-10-05/pdf/00-25500.pdf
- "Physician Medical Identity Theft" by S. Agrawal and P. Budetti in the "Journal of the American Medical Association," Volume 307, Number 5, Pages 459 – 460 (February 1, 2012) http://jama.jamanetwork.com/article.aspx?articleid=1104942
- "Physician Sentenced to Eight Years in Federal Prison for Role in Massive Medicare Fraud Scam," press release by the U.S. Department of Justice (January 12, 2012) http://www.fbi.gov/sacramento/press-releases/2012/physician-sentenced-to-eight-years-in-federal-prison-for-role-in-massive-medicare-fraud-scam
- "Policy Basics: Where Do Our Federal Tax Dollars Go?" by the Center on Budget and Policy Priorities (April 12, 2013) http://www.cbpp.org/cms/?fa=view&id=1258
- "Preventing and Detecting Physician Medical Identity Theft" by S. Agrawal, Centers for Medicare & Medicaid Services, Center for Program Integrity (February 13, 2012; Retrieved March 20, 2012)
- "Sarasota County Woman Sentenced For Health Care Fraud," press release by the U.S. Attorney's Office, Middle District of Florida (January 5, 2012) http://www.justice.gov/usao/flm/press/2012/jan/20120105_Matchin.html
- Tamper Resistant Prescriptions http://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/FraudAbuseforProfs/TRP.html
- HHS-OIG. (March 13, 2012). Office of Investigations Representative.

1. Centers for Medicare & Medicaid Services. Retrieved February 13, 2012, from http://www.cms.gov
2. Center on Budget and Policy Priorities. (2013, April 12). "Policy Basics: Where Do Our Federal Tax Dollars Go?" Retrieved February 24, 2014, from http://www.cbpp.org/cms/?fa=view&id=1258
3. Federal Trade Commission. (February 2010). "Consumer Sentinel Network Data Book for January-December 2009." Retrieved April 5, 2012, from http://www.ftc.gov/sites/default/files/documents/reports_annual/sentinel-cy-2009/sentinel-cy2009.pdf

The Medicare Learning Network® (MLN), a registered trademark of CMS, is the brand name for official information health care professionals can trust. For additional information, visit the MLN's web page at http://go.cms.gov/MLNGenInfo on the CMS website.

Check out CMS on: