

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



Medicaid Program Integrity: Preventing Provider Medical Identity Theft



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 and help them protect their medical identities. “Medical identity theft is 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.”

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.

Common Provider Medical Identity Theft Schemes

A common provider medical identity theft scheme involves a fraudster billing services directly in a physician’s or other provider’s name even though the clinician never provided the service. Another common scheme involves using physician and other provider medical identifiers to refer patients for additional services and supplies, such as home health services, diagnostic testing, and medical equipment and supplies.

Medicaid Program Integrity: Preventing Provider Medical Identity Theft



Main Provider Risk Factors

The primary risk factor for medical identity theft is provider participation in fraud schemes. Providers who allow misuse of their identifiers place this information at significant risk for subsequent theft and can create unintended consequences. Common examples of providers allowing the misuse of medical identifiers include signing:

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

Purposeful misuse of medical identifiers can lead to significant consequences, such as civil monetary penalties, criminal fines and restitution, prison time, and exclusion from Medicare and Medicaid. Physicians (and other providers) can be held liable for these actions even without evidence of other fraud.

Also, inherent structural risks are associated with provider medical identifiers, such as public access to National Provider Identifiers (NPIs) and provider license numbers. Other risks include an organization's expectation for providers to disclose identifiers when they apply for a position. The more parties with access to a provider's medical identifiers, the greater the risk of exposure for medical identity theft. Examples of high-risk exposure include:

- Allowing mid-level practitioners the use of medical identifiers;
- Providing medical identifiers to staff; and
- Reassigning medical identifiers for billing purposes.

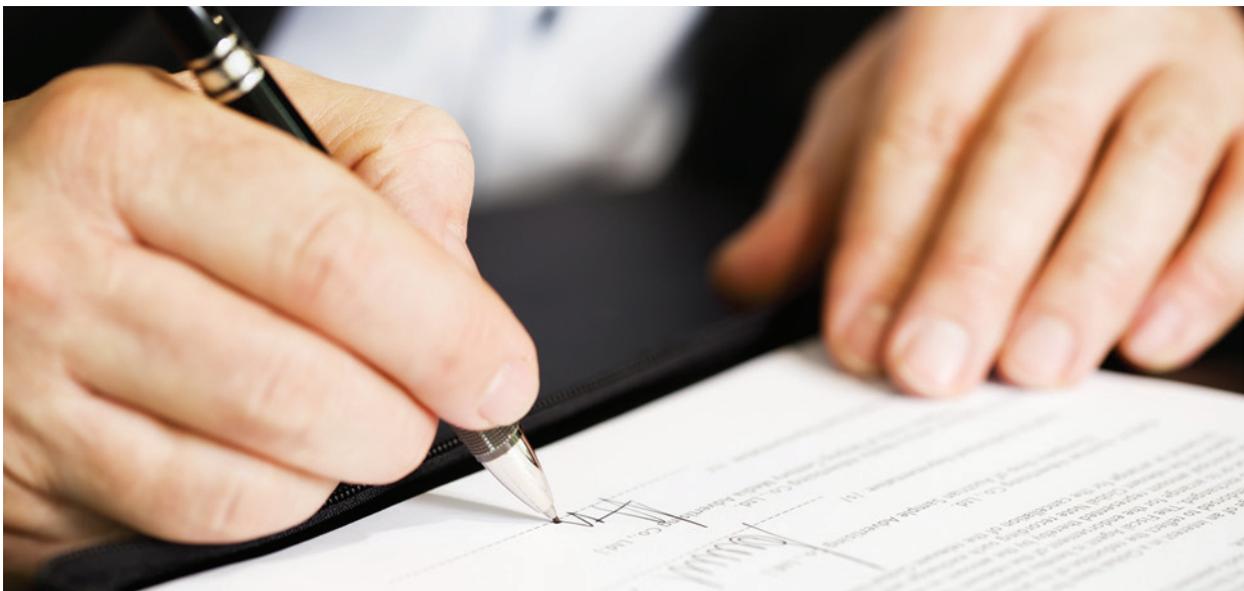


Medicaid Program Integrity: Preventing Provider Medical Identity Theft

Mitigate Risk

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:

- **Actively managing enrollment information with payers** by updating enrollment changes especially when:
 - Changing banking information;
 - Opening, closing, or moving practice locations; and
 - Separating from an organization.
- **Controlling unique medical identifiers** by taking steps, such as:
 - Keeping track of all prescription pads;
 - Screening employees;
 - Securing all information technology; and
 - Thoroughly training staff on all policies and procedures.
- **Engaging patients in conversation about the risks of medical identity theft** by:
 - Explaining the impact it can have on them and their medical records;
 - Looking for signs of potential identity theft; and
 - Warning patients of the dangers of card sharing.
- **Monitoring billing and compliance processes** by strengthening policies and procedures to minimize risks and improve overall program integrity. Policies and procedures might include:
 - Adopting sound billing practices (for example, reviewing remittance notices);
 - Carefully reading documents before signing them; and
 - Limiting and monitoring third party use of medical identifiers.



Medicaid Program Integrity: Preventing Provider Medical Identity Theft

Remediation for Victims

The goals of Center for Program Integrity (CPI) include proactively identifying and helping identity theft victims. CPI can:

- Help absolve the financial problems related to the theft, such as overpayments and tax obligations; and
- Respond to the needs of legitimate providers.

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. For additional information about CPI, refer to <http://www.cms.gov/Medicare-Medicaid-Coordination/Fraud-Prevention/MedicaidIntegrityProgram/downloads/cpiinitiatives.pdf> on the CMS website.

Report It

Report suspected medical identity theft to:

- **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>
- **U.S. Department of Health & Human Services (HHS), Office of Inspector General (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.



Medicaid Program Integrity: Preventing Provider Medical Identity Theft



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) credits. Please note, you **must** register and complete a post-assessment test and evaluation to receive Continuing Education Units (CEUs) or Continuing Medical Education (CME) credits 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.
- For information on how to report fraud, visit <http://oig.hhs.gov/fraud> on the Internet.



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

- “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>
- “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)

Medicaid Program Integrity: Preventing Provider Medical Identity Theft



This fact sheet 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 fact sheet was prepared as a service to the public and is not intended to grant rights or impose obligations. This fact sheet 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 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.

Check out CMS on:

