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 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 pay[o]rs for fraudulent medical goods or services.”[1]

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 is 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.[2]

Main Provider Risk Factors

The primary risk factor for medical identity theft is provider complicity in fraud schemes. Providers who voluntarily permit misuse of their identifiers place this information at significant risk for subsequent theft and can create unintended consequences. Common examples of ways providers allow the misuse of medical identifiers include signing referrals for patients they do not know, signing Certificates of Medical Necessity (CMNs) for patients who do not need the service or supply, signing CMNs for more than what patients actually need, and even signing blank referral forms. 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.[3]

In addition to provider complicity and the voluntary misuse of medical identifiers, inherent structural risks are associated with provider medical identifiers, such as public access to National Provider Identifiers and provider license numbers. Other risks include the expectation by an organization for providers to disclose identifiers at the time of application 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 reassigning medical identifiers for billing purposes, providing medical identifiers to staff, and allowing mid-level practitioners the use of medical identifiers.

Mitigate Risk

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 payors by updating enrollment changes especially when opening, closing, or moving practice locations; when separating from an organization; or when changing banking information;
- 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;
- Controlling unique medical identifiers by taking steps, such as thoroughly training staff on all policies and procedures, screening employees, securing all information technology, and keeping track of all prescription pads; and
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.

**Remediation for Victims**

The Center for Program Integrity’s (CPI) goal is to proactively identify and help identity theft victims. CPI can:

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

For additional CPI information, visit [https://www.cms.gov/MedicaidIntegrityProgram/Downloads/cpiinitiatives.pdf](https://www.cms.gov/MedicaidIntegrityProgram/Downloads/cpiinitiatives.pdf) on the CMS website.

**Report It**

Report suspected medical identity theft to local law enforcement services; the State Medicaid agency where you practice; the Federal Trade Commission; the U.S. Department of Health and Human Services, Office of Inspector General (HHS-OIG); and your Health and Human Services regional office.

**Resources**

For more information about medical identity theft, visit [https://cms.meridianksi.com/kc/main/pop_up_frm.asp?loc=/kc/ilc/course_info_enroll_info.asp%3Fpreview%3Dfalse%26crs_ident%3DC00137](https://cms.meridianksi.com/kc/main/pop_up_frm.asp?loc=/kc/ilc/course_info_enroll_info.asp%3Fpreview%3Dfalse%26crs_ident%3DC00137) to review a “Safeguarding Your Medical Identity” Continuing Medical Education (CME) webinar and to download the “Safeguarding Your Medical Identity CME Program References and Resources” handout. The handout includes a list of websites and additional sources of helpful information. Information on how to report fraud can be found by visiting [https://forms.oig.hhs.gov/hotlineoperations/notthsemployeeen.aspx](https://forms.oig.hhs.gov/hotlineoperations/notthsemployeeen.aspx) on the HHS-OIG website.

**Disclaimer**

This fact sheet 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 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. 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.

March 2014