



---

---

---

---

---

---

---

---

### Speakers

- Shantanu Agrawal, M.D., Medical Director, Center for Program Integrity, Centers for Medicare and Medicaid Services, U.S. Department of Health and Human Services
- Julie Taitzman, M.D., Chief Medical Officer, Office of Inspector General, U.S. Department of Health & Human Services

Centers for Medicare & Medicaid Services 2

---

---

---

---

---

---

---

---

### Objective

At the conclusion of this presentation, participants will be able to:

- Recognize the scope of the problem of medical identity theft and strategies for mitigating it

Centers for Medicare & Medicaid Services 3

---

---

---

---

---

---

---

---

### Goals

- Describe medical identity theft and the associated problems
- Recognize the risks for medical identity theft
- List strategies for mitigating vulnerability to medical identity theft
- List resources for reporting medical identity theft

Centers for Medicare & Medicaid Services 4

---

---

---

---

---

---

---

---

### Dr. Peters' Tale of Identity Theft

- Stolen credentials
- False claims billed in her name



Centers for Medicare & Medicaid Services 5

---

---

---

---

---

---

---

---

### Secretary Kathleen Sebelius U.S. Department of Health and Human Services

"Dr. Peters was simply doing what she loved, treating her patients and providing care to those in need."



Centers for Medicare & Medicaid Services 6

---

---

---

---

---

---

---

---

### Medicaid, Medicare, and CHIP

- Millions of participating physicians and other providers furnish services through Medicare, Medicaid, and the Children's Health Insurance Program (CHIP)
- These programs provide health care coverage for 100 million people
- One out of every four Americans receives health care services from a public health care program

Centers for Medicare & Medicaid Services

7

---

---

---

---

---

---

---

---

### Eric Holder, Attorney General of the United States

"In communities across the region, our health care system is under siege—exploited by criminals intent on lining their own pockets..."



Centers for Medicare & Medicaid Services

8

---

---

---

---

---

---

---

---

### What Is Medical Identity Theft?

"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."

Centers for Medicare & Medicaid Services

9

---

---

---

---

---

---

---

---

### Scope of the Issue

- Both the Federal Trade Commission (FTC) and the Centers for Medicare & Medicaid Services (CMS) track cases of provider and patient medical identity theft
- Latest FTC data shows that more than 3,600 physician and patient cases were reported in 2009
- Many cases of medical identity theft may go unreported

Centers for Medicare & Medicaid Services 10

---

---

---

---

---

---

---

---

### Case Study #1: Fraudulent Prescriptions

- 250 forged narcotics prescriptions
- Multiple co-conspirators
- Used pharmacies throughout the State
- Stolen Medicaid cards



Centers for Medicare & Medicaid Services 11

---

---

---

---

---

---

---

---

### Case Study #1: Lessons Learned

- Keep track of prescription pads
- Beneficiaries may not know their ID has been stolen
- Educate the beneficiary



Centers for Medicare & Medicaid Services 12

---

---

---

---

---

---

---

---

### True or False?

“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.”

- Physicians/providers: National Provider Identifier (NPI), Tax Identification Number (TIN), medical licensure
- Patients: Health Insurance Claim Number (HICN), insurance ID card

---

---

---

---

---

---

---

---

### Center for Program Integrity Mission and Activities

The central purpose and role of the Center for Program Integrity (CPI) is to ensure the correct payments are made to legitimate providers for covered appropriate and reasonable services for eligible beneficiaries of the Medicare and Medicaid programs. Program integrity encompasses a range of activities to target the various causes of improper payments.




---

---

---

---

---

---

---

---

### Compromised Numbers Database —How Numbers Are Added

1. CPI and contractors’ proactive data analysis
2. Beneficiary complaints of suspect billings
3. Physician complaints after reviewing reports
4. Interviews with providers and beneficiaries
5. Law enforcement investigations
6. Reports from other CMS programs

---

---

---

---

---

---

---

---

### Compromised Medical Identifiers

CPI has identified:

- ~5,000 compromised Medicare provider numbers (Parts A/B/D)
- ~280,000 compromised beneficiary numbers

CMS is working to improve risk stratification and categorization of numbers by victim or perpetrator.

---

---

---

---

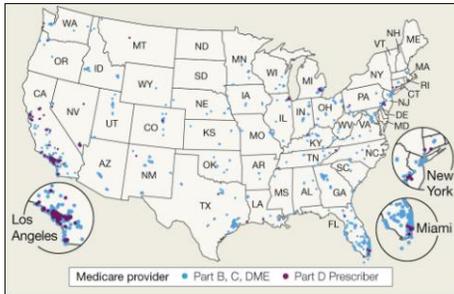
---

---

---

---

### Geographic Distribution of Compromised Medical Identifiers



JAMA. 2011;307(5):459-460. © American Medical Association

---

---

---

---

---

---

---

---

### True or False?

CPI is currently tracking thousands of compromised physician and patient medical identifiers.

---

---

---

---

---

---

---

---

### Ways of Misusing Physician Identifiers —Referrals

Criminals can use stolen Medicaid identifiers in numerous ways. One of the most common schemes used to commit fraud is using physician medical identifiers to refer patients for additional services or supplies.



---

---

---

---

---

---

---

---

### Case Study #2: Patient Recruiting Scheme

- Patient recruiter hired to obtain patient information and identities
- Medicare beneficiaries and legitimate physicians approached for unnecessary services
- If that failed, unrelated physicians were utilized to order services using stolen identities and the original stolen patient identities

---

---

---

---

---

---

---

---

### Case Study #2: Lessons Learned

- Consider medical necessity before authorizing services
- Perform all necessary exams and testing before authorizing related services
- Set internal policies to avoid taking shortcuts



---

---

---

---

---

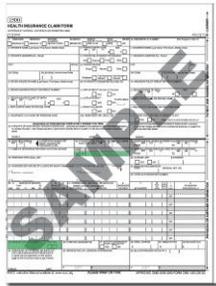
---

---

---

### Ways of Misusing Physician Identifiers —Directly Billing Services

Another common scheme using stolen physician identifiers involves directly billing services in a physician's name, as if the physician whose identity was stolen actually performed those services.



---

---

---

---

---

---

---

---

---

---

### Learning Check: Methods

#### Direct Billing

- Fraudster bills directly for services in the physician's name
  - Examples: billings include professional services or evaluation and management
- Results in financial harm to the physician and potentially generates overpayments

#### Ordering/Referring

- Physician's information used to order or refer services
  - Examples: laboratory analyses, diagnostic testing, durable medical equipment
- Difficult to detect

---

---

---

---

---

---

---

---

---

---

### Consequences of Stolen Physician Identifiers

- Overpayment demand letters
- Tax liabilities
- Credit issues
- Difficulty exonerating themselves
- Damaged reputation



---

---

---

---

---

---

---

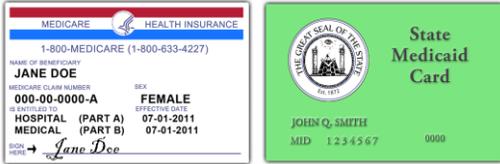
---

---

---

### Misusing Beneficiary Identifiers

One of the most common beneficiary medical identity theft schemes involves the theft of a beneficiary's medical identifiers for billing purposes or obtaining services.



---

---

---

---

---

---

---

---

---

---

### Case Study #3: Beneficiary Direct Billing Scheme

- Trafficking beneficiary information
- Relative medical identity theft
- Soliciting beneficiary information

---

---

---

---

---

---

---

---

---

---

### Case Study #3: Lessons Learned

- Patients should be educated to protect their Medicaid and Medicare cards
- Cards and patient information should not be shared with anyone, including family members
- Stolen identifiers can corrupt the medical record of the victimized patient



---

---

---

---

---

---

---

---

---

---

### Consequences of Stolen Beneficiary Identifiers

Consequences can include:

- Compromised patient care
- Denial of services
- Financial obligations

"I wasn't getting the nursing care I needed, and services were being cut back because of me being over the so-called spending limit."  
— Richard West

Centers for Medicare & Medicaid Services 28

---

---

---

---

---

---

---

---

### Learning Check: Consequences

**Physicians**

- Impacts all utilization reviews, such as comparative billing reports, quality measurement, and reporting
- Financial or tax liabilities from fraudulent billing
- Accountability for care or services they did not provide

**Patients**

- Increases in copays or insurance costs
- Inability to get coverage or services that duplicate fraudulent billing
- Safety may be placed at risk through alteration of the medical record

Centers for Medicare & Medicaid Services 29

---

---

---

---

---

---

---

---

### Physician Risk Factors

The primary risk factor that physicians can control for medical identity theft is complicity in fraud schemes. Physicians who voluntarily permit misuse of their identities place this information at significant risk for subsequent theft.

Centers for Medicare & Medicaid Services 30

---

---

---

---

---

---

---

---

### Case Study #4: Voluntary Medical Identifier Misuse Scheme

- Physician co-owner and complicit in the scheme
- No treatment provided by the physician
- He signed off on fraudulently ordered treatments and billings



Centers for Medicare & Medicaid Services 31

---

---

---

---

---

---

---

---

### Case Study #4: Lessons Learned

- Accurate medical record documentation is important and supports medical necessity
- Only bill and chart for the services provided
- Certify only those claims relevant to the services provided



Centers for Medicare & Medicaid Services 32

---

---

---

---

---

---

---

---

### True or False?

Complicity in fraud schemes is the primary risk factor for medical identity theft.

Centers for Medicare & Medicaid Services 33

---

---

---

---

---

---

---

---

### Beneficiary Risk Factors

Card sharing is a common complicit beneficiary medical identity theft scheme.

- 26% of surveyed respondents admitted sharing their medical identifiers
- Respondents were most likely to share with family members
- Cards were shared because family members had no insurance or could not afford needed treatment

---

---

---

---

---

---

---

---

### Public Access to Physician Medical Identifiers

Public access to physician identifiers, such as:

- National Provider Identifier (NPI)
- Tax Identification Number (TIN)
- U.S. Drug Enforcement Administration (DEA) number
- State license number
- Job applications

---

---

---

---

---

---

---

---

### Making Medical Identifiers Available

Physicians working with multiple organizations are at particular risk for theft or misuse of identifiers.



---

---

---

---

---

---

---

---

### Case Study #5: Medical Identifier Exposure Scheme

- Fraud perpetrator recruited physicians to be “Medical Directors”
- Physicians were rarely present at the clinic but allowed false documentation and billing by mid-level providers
- Mid-level providers were complicit—and, importantly, so were the physicians



Centers for Medicare & Medicaid Services

37

---

---

---

---

---

---

---

---

### Case Study #5: Lessons Learned

- If it sounds too good to be true, it probably is
- Be acquainted with all business partners
- Determine how much time the position will require
- Monitor the use of identifiers



Centers for Medicare & Medicaid Services

38

---

---

---

---

---

---

---

---

### Mitigating Risks

1. Actively manage enrollment information with payors
2. Monitor billing and compliance processes
3. Control unique medical identifiers
4. Engage patients about identity theft

Centers for Medicare & Medicaid Services

39

---

---

---

---

---

---

---

---

### Actively Manage Enrollment Information

Actively manage enrollment information with payors by updating:

- Practice locations—especially when opening, closing, or moving locations
- All organization separations
- Electronic funds transfer locations

---

---

---

---

---

---

---

---

### Monitor

Monitor billing and compliance processes by:

- Being aware of billings in your name
- Paying attention to the organizations and mid-level practitioners to whom billing privileges are assigned
- Actively reviewing organization remittance notices and comparing them to documentation
- Ensuring charting supports billed services
- Reading all documents before signing

If you suspect fraud, report it!

---

---

---

---

---

---

---

---

### Control

Control unique medical identifiers.

- Take the time to learn about an organization before sharing medical identifiers
- Train staff to protect identifiers
  - Question unknown individuals who contact the office asking for medical identifiers
  - Carefully consider which staff will have access to medical identifiers

---

---

---

---

---

---

---

---

### Control Continued

#### Control unique medical identifiers:

- Screen employees—take appropriate action
  - Ensure employees are not excluded from participation <https://oig.hhs.gov/exclusions/index.asp> and <https://www.sam.gov/portal/public/SAM/#1>
  - Ensure all background checks adhere to State Medicaid rules and regulations
- Control prescription pads
  - Ensure prescription pads are not inadvertently left unattended
  - Completely fill out prescriptions and other documents to prevent tampering
- Secure technology
  - Maintain the integrity of computer log-ons
  - Authenticate all system users

---

---

---

---

---

---

---

---

### Engage Patients

Physicians and other providers are in an excellent position to raise patient awareness by engaging and educating them about medical identity theft.

- Educate patients about the risks of card sharing
- Educate patients to request medical bills



---

---

---

---

---

---

---

---

### True or False?

Identity theft may be mitigated when a physician actively manages enrollment information with payors, monitors billing and compliance processes, controls unique medical identifiers, and engages patients about identity theft.

---

---

---

---

---

---

---

---

### Identity Remediation Process

CPI's goal is to proactively identify and help victims. The staff at CPI is working hard to assist victims of identity theft. CPI can:

- Help absolve related debts—overpayments and tax obligations
- Respond to the needs of legitimate providers
- <https://www.cms.gov/MedicaidIntegrityProgram/Downloads/cpiinitiatives.pdf>

---

---

---

---

---

---

---

---

### Report It!

Victims of medical identity theft can and should report it to the:

- Local law enforcement service
- State Medicaid agency (SMA) where you practice
- FTC
- HHS-OIG
- Health and Human Services regional office

---

---

---

---

---

---

---

---

### Conclusion

Medical identity theft is a problem for physicians. Safeguard your medical identity by:

- Recognizing the scope of the problem
- Educating yourself and your staff
- Implementing mitigating strategies
- Reporting it

---

---

---

---

---

---

---

---

## Contacts

- SMA—Visit <https://www.cms.gov/FraudAbuseforConsumers/Downloads/smafraudcontacts.pdf> on the CMS website. Click on the state where you practice for the appropriate contact information, and then notify the agency
- 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 #: 1-866-653-4261  
Website: <http://www.ftc.gov/bcp/edu/microsites/idtheft/>
- HHS-OIG Hotline and report suspected fraud:  
Phone: 1-800-447-8477 (1-800-HHS-TIPS)  
TTY #: 1-800-377-4950  
Fax #: 1-800-223-8164  
E-mail: [HSSTips@oig.hhs.gov](mailto:HSSTips@oig.hhs.gov)  
Website: <http://oig.hhs.gov/fraud/report-fraud/index.asp>

---

---

---

---

---

---

---

---

---

---

---

---

## HHS-OIG Compliance Guidance



Visit <http://oig.hhs.gov/compliance/compliance-guidance/index.asp> on the HHS-OIG website.

---

---

---

---

---

---

---

---

---

---

---

---

## Disclaimer

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

---

---

---

---

---

---

---

---

---

---

---

---