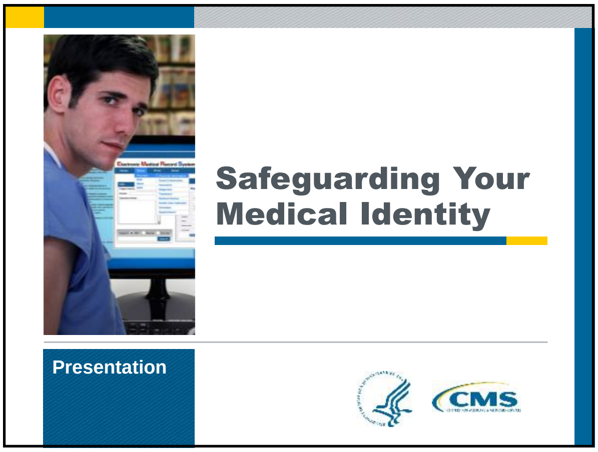
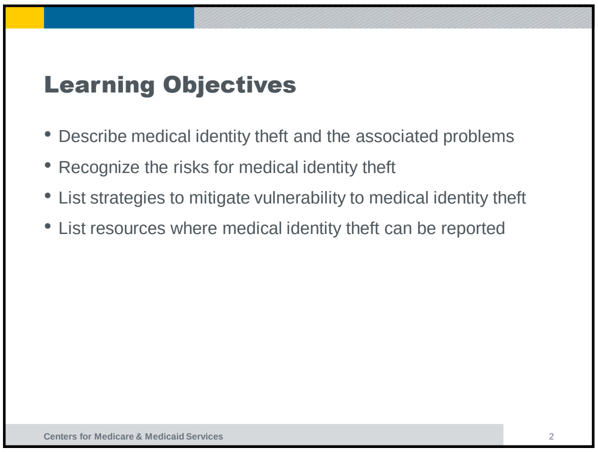


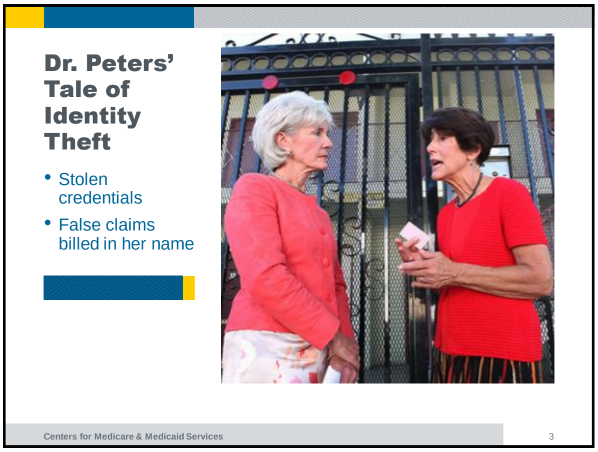
Safeguarding Your Medical Identity

Presentation



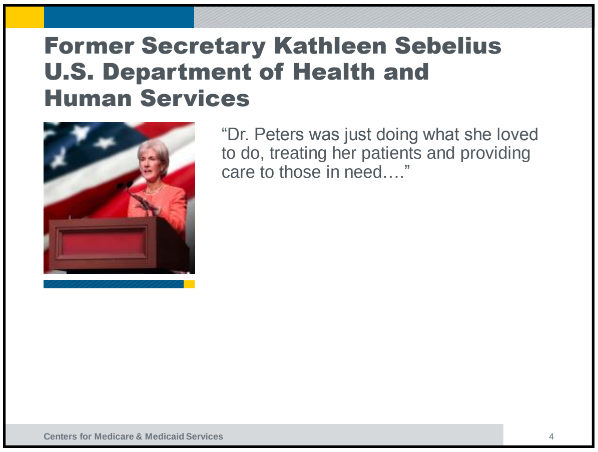
Learning Objectives

- Describe medical identity theft and the associated problems
- Recognize the risks for medical identity theft
- List strategies to mitigate vulnerability to medical identity theft
- List resources where medical identity theft can be reported



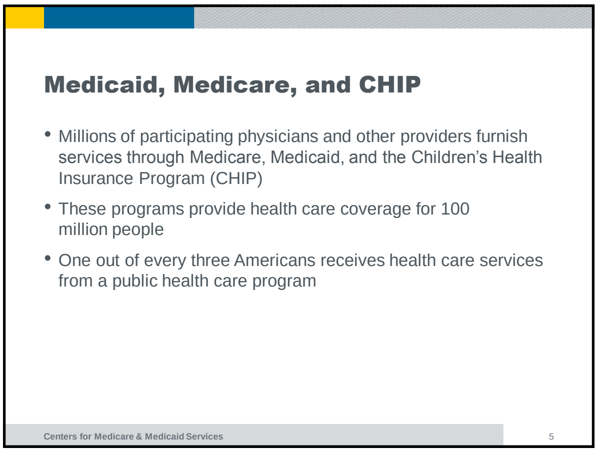
Dr. Peters' Tale of Identity Theft

- Stolen credentials
- False claims billed in her name



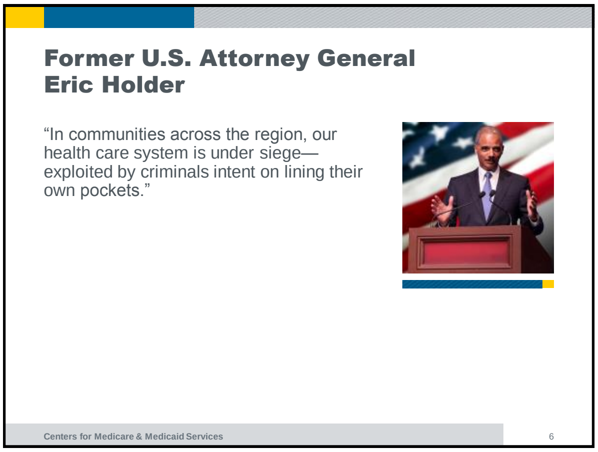
Former Secretary Kathleen Sebelius U.S. Department of Health and Human Services

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



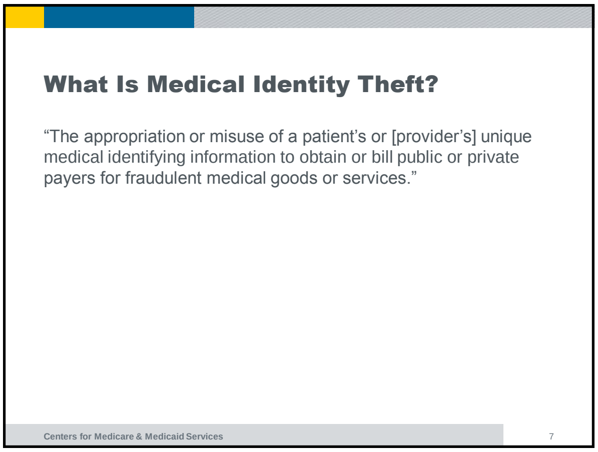
Medicaid, Medicare, and CHIP

- 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 three Americans receives health care services from a public health care program



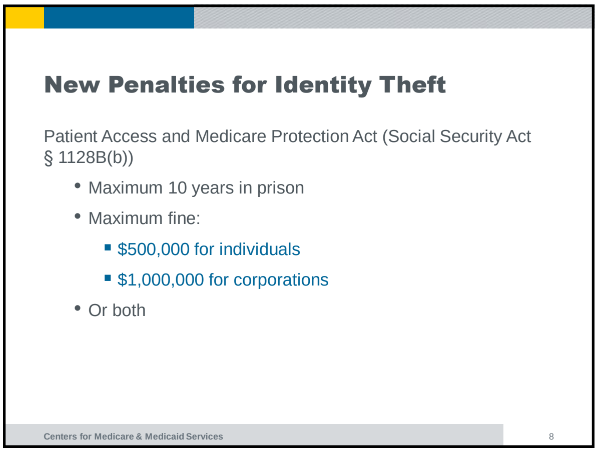
Former U.S. Attorney General Eric Holder

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



What Is Medical Identity Theft?

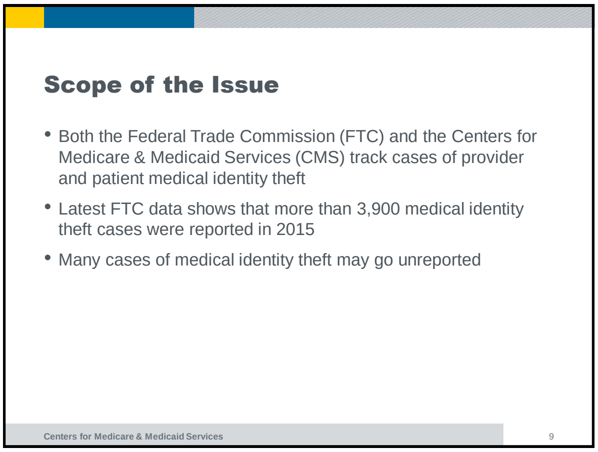
"The appropriation or misuse of a patient's or [provider's] unique medical identifying information to obtain or bill public or private payers for fraudulent medical goods or services."



New Penalties for Identity Theft

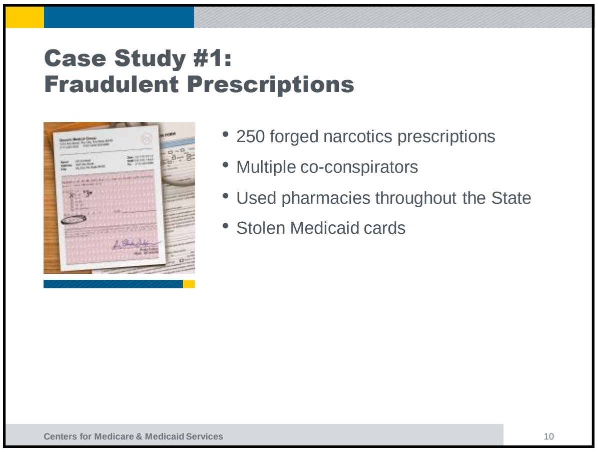
Patient Access and Medicare Protection Act (Social Security Act § 1128B(b))

- Maximum 10 years in prison
- Maximum fine:
  - $500,000 for individuals
  - $1,000,000 for corporations
- Or both



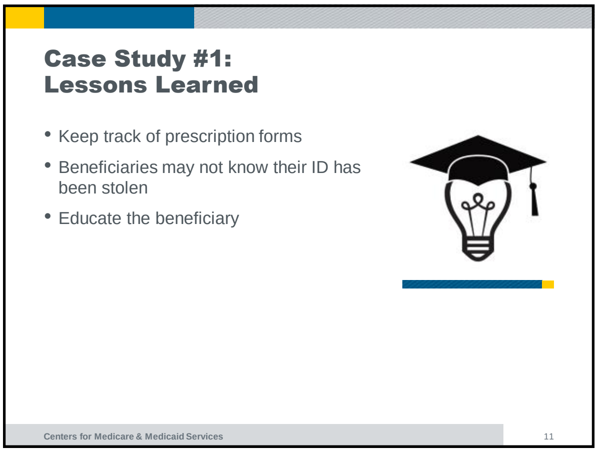
Scope of the Issue

- 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 3,900 medical identity theft cases were reported in 2015
- Many cases of medical identity theft may go unreported



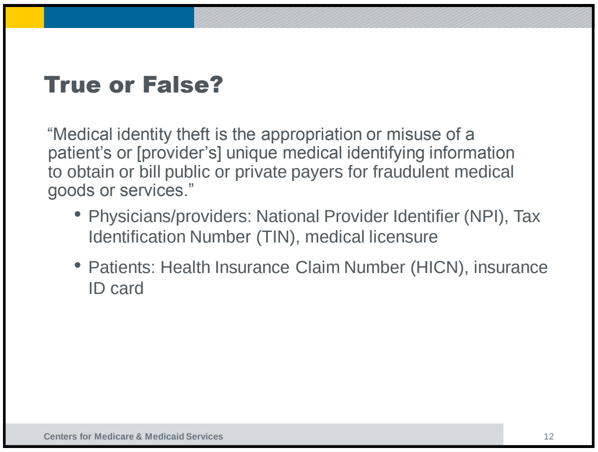
Case Study #1: Fraudulent Prescriptions

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



Case Study #1: Lessons Learned

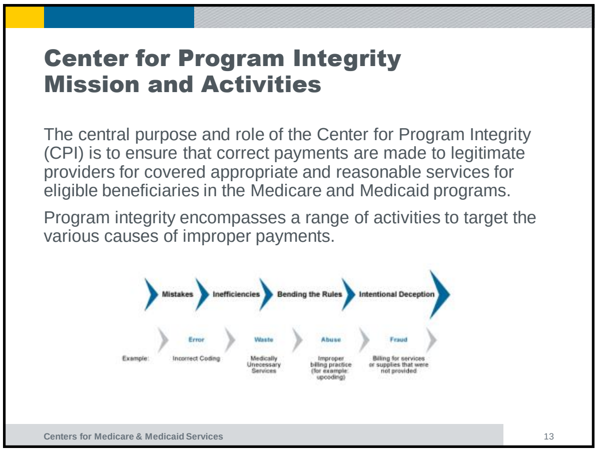
- Keep track of prescription forms
- Beneficiaries may not know their ID has been stolen
- Educate the beneficiary



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 payers 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



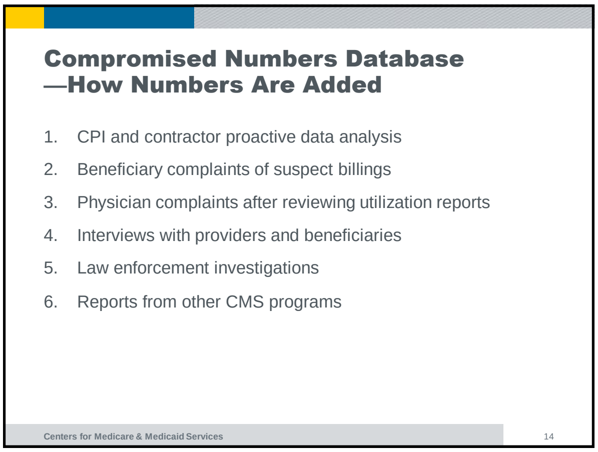
Center for Program Integrity Mission and Activities

The central purpose and role of the Center for Program Integrity (CPI) is to ensure that correct payments are made to legitimate providers for covered appropriate and reasonable services for eligible beneficiaries in the Medicare and Medicaid programs.

Program integrity encompasses a range of activities to target the various causes of improper payments.

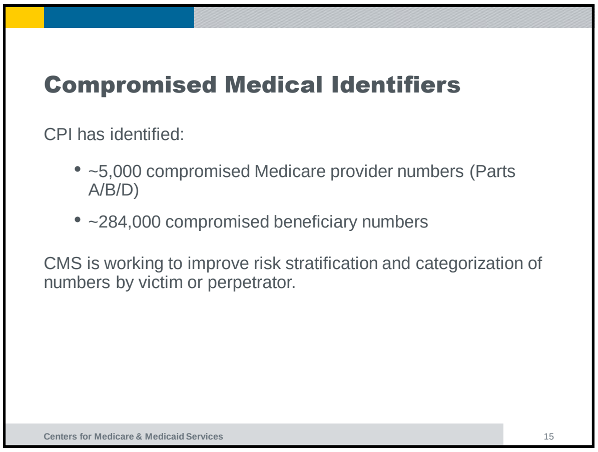
Mistakes
Inefficiencies
Bending the Rules
Intentional Deception

Example:
Error
Incorrect Coding
Waste
Medically Unecessary Services
Abuse
Improper billing practice (for example: upcoding)
Fraud
Billing for services or supplies that were not provided



Compromised Numbers Database —How Numbers Are Added

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

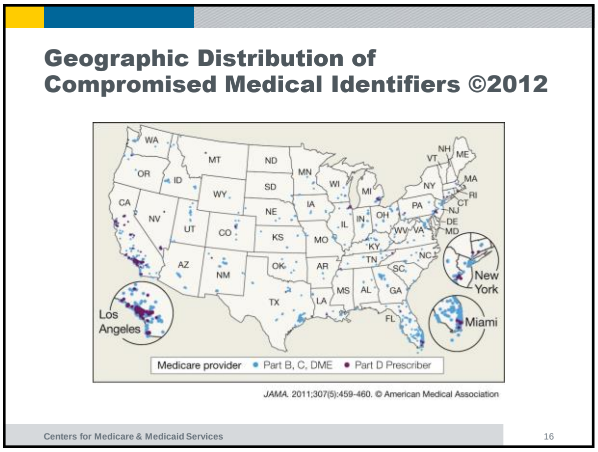


Compromised Medical Identifiers

CPI has identified:

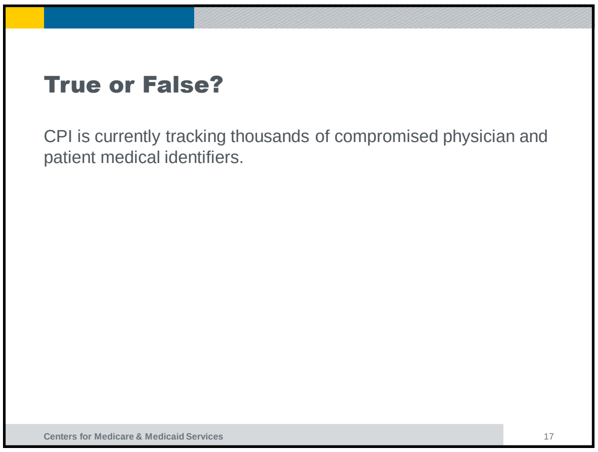
- ~5,000 compromised Medicare provider numbers (Parts A/B/D)
- ~284,000 compromised beneficiary numbers

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



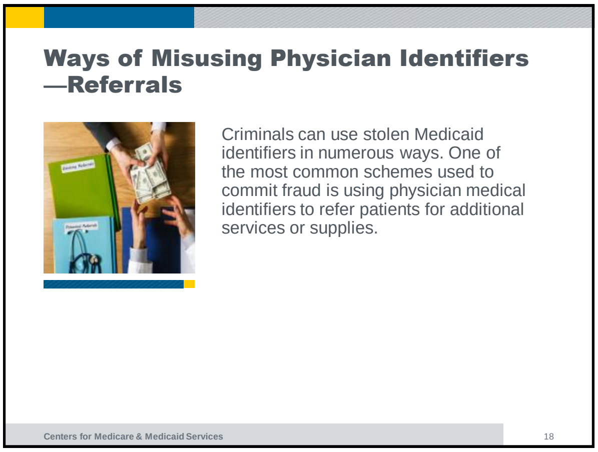
Geographic Distribution of Compromised Medical Identifiers ©2012

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 tests 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 provided the 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

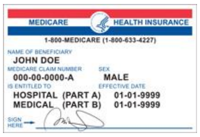
- Physician's information used to order or refer services
  - Examples: laboratory analyses, diagnostic tests, durable medical equipment (DME)
- Difficult to detect

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.



MEDICARE HEALTH INSURANCE

1-800-MEDICARE (1-800-633-4227)

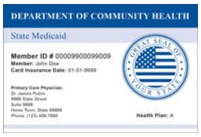
NAME OF BENEFICIARY
JOHN DOE

MEDICARE CLAIM NUMBER 000-00-0000-A

SEX MALE

IS ENTITLED TO / EFFECTIVE DATE
HOSPITAL (PART A) 01-01-9999
MEDICAL (PART B) 01-01-9999

SIGN HERE →



DEPARTMENT OF COMMUNITY HEALTH

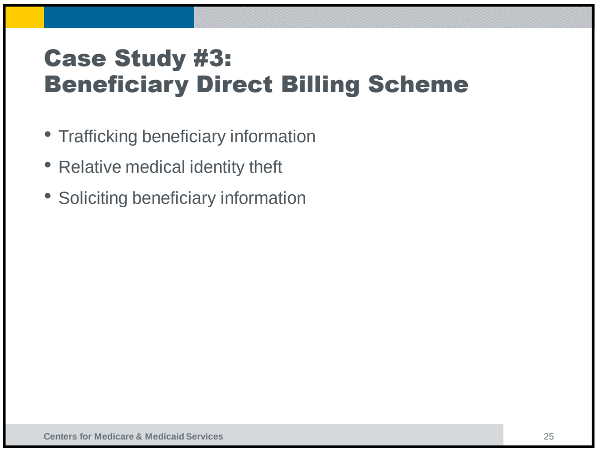
State Medicaid

Member ID # 00009900099009
Member: John Doe
Card Insurance Date: 01-01-9999

Primary Care Physician:
Dr. James Public
9999 State Street
Suite 9999
Home Town, State 99999
Phone: (123) 456-7890

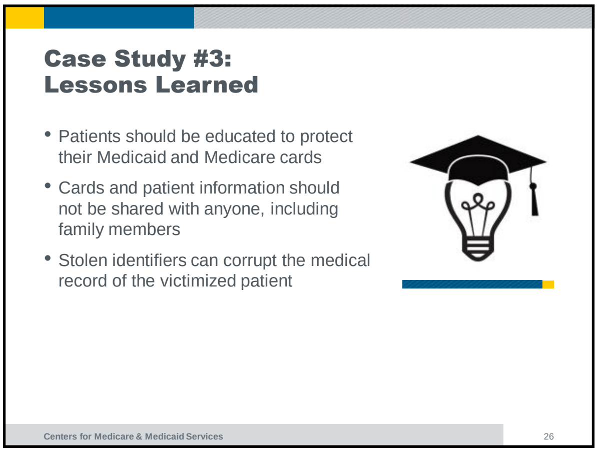
Health Plan: A

GREAT SEAL OF YOUR STATE



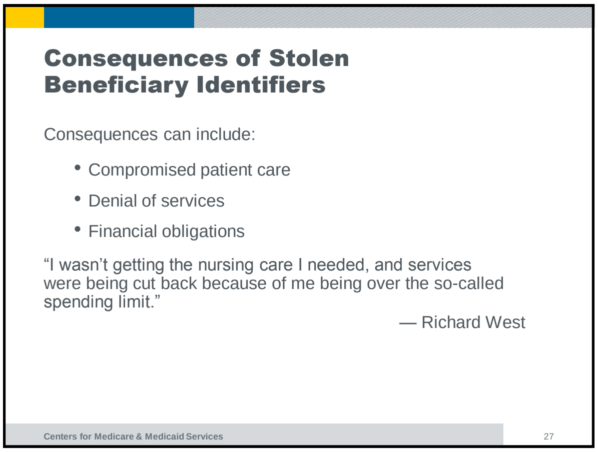
Case Study #3: Beneficiary Direct Billing Scheme

- 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



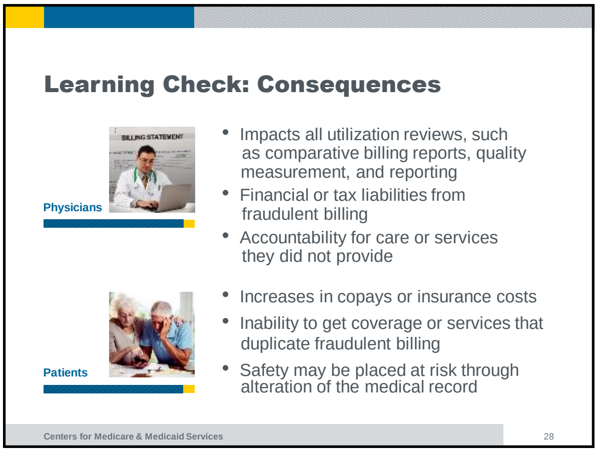
Consequences of Stolen Beneficiary Identifiers

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



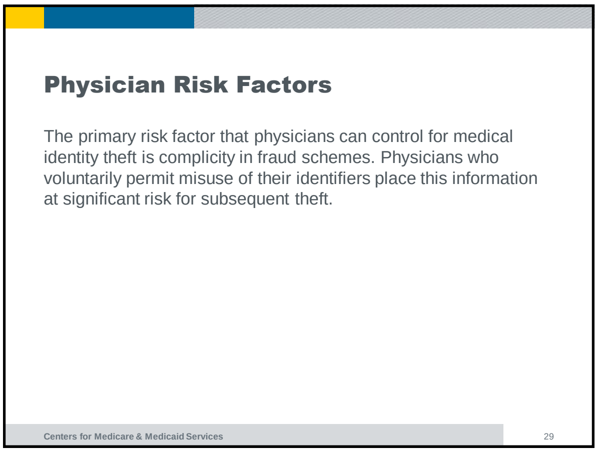
Learning Check: Consequences

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

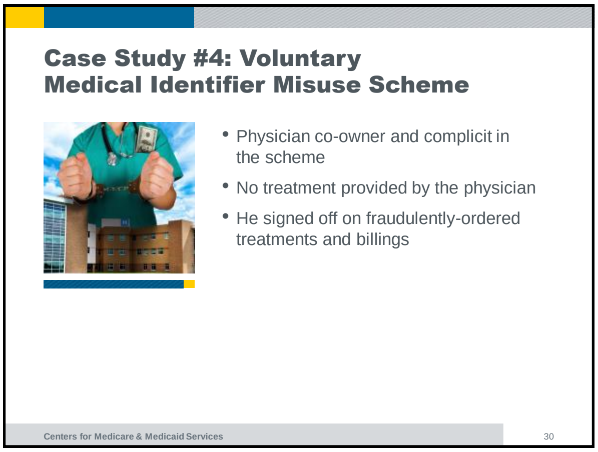
Patients

- 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



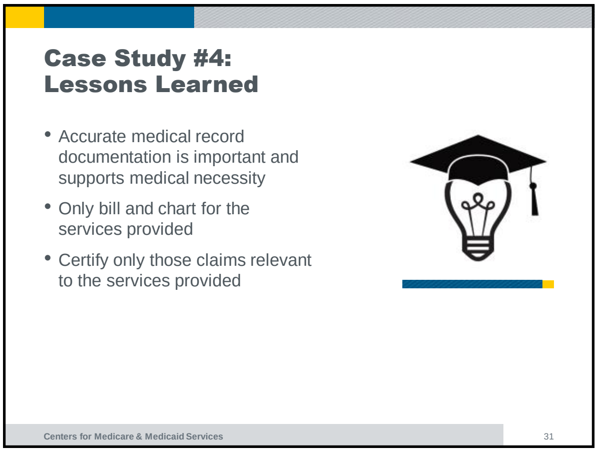
Physician Risk Factors

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



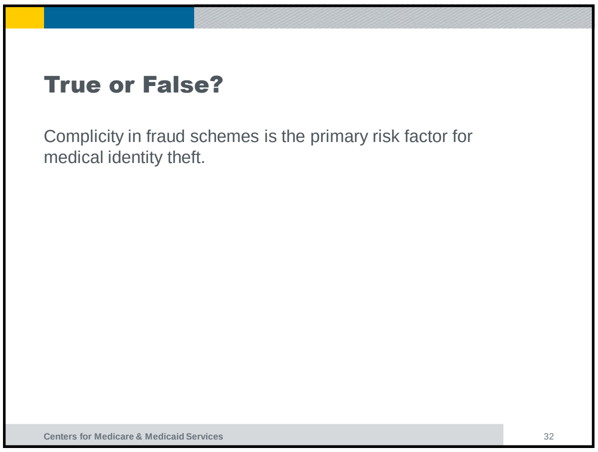
Case Study #4: Voluntary Medical Identifier Misuse Scheme

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



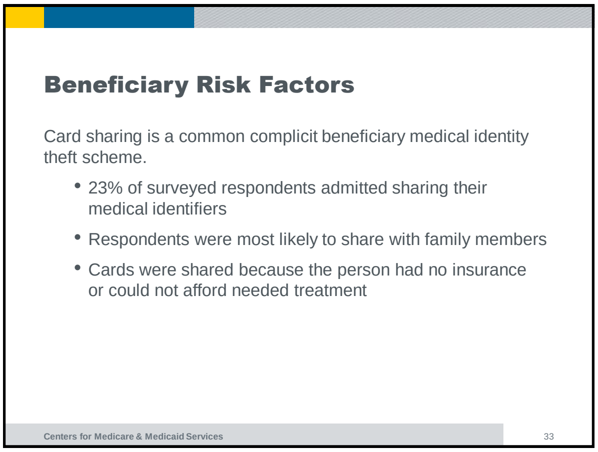
Case Study #4: Lessons Learned

- 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



True or False?

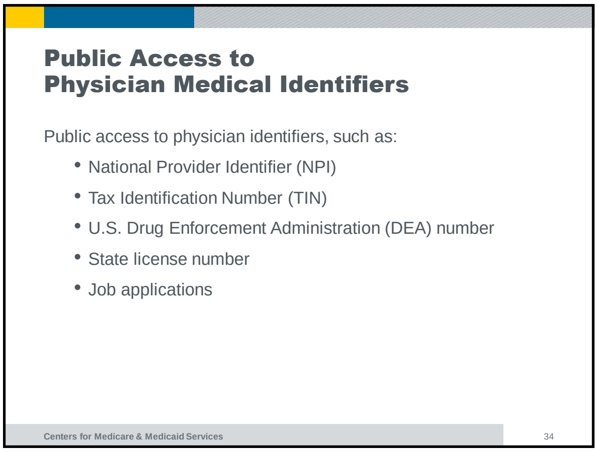
Complicity in fraud schemes is the primary risk factor for medical identity theft.



Beneficiary Risk Factors

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

- 23% of surveyed respondents admitted sharing their medical identifiers
- Respondents were most likely to share with family members
- Cards were shared because the person had no insurance or could not afford needed treatment

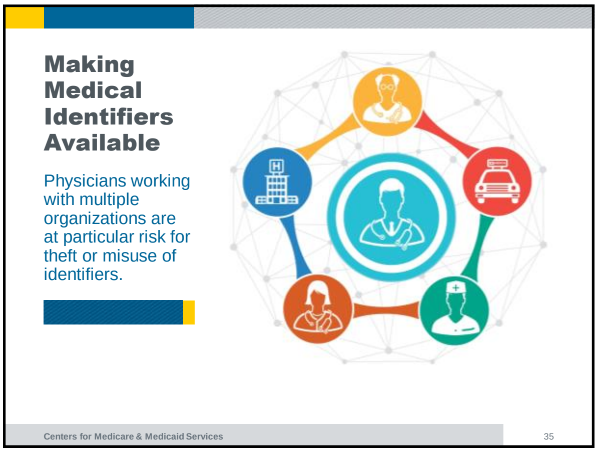


Public Access to Physician Medical Identifiers

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

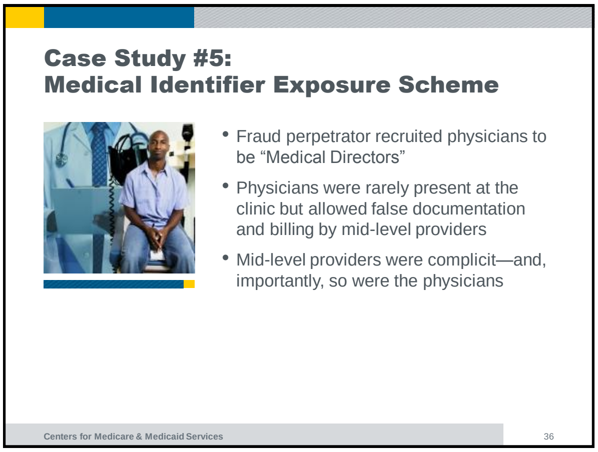
Centers for Medicare & Medicaid Services 34



Making Medical Identifiers Available

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

Centers for Medicare & Medicaid Services 35



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 36

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

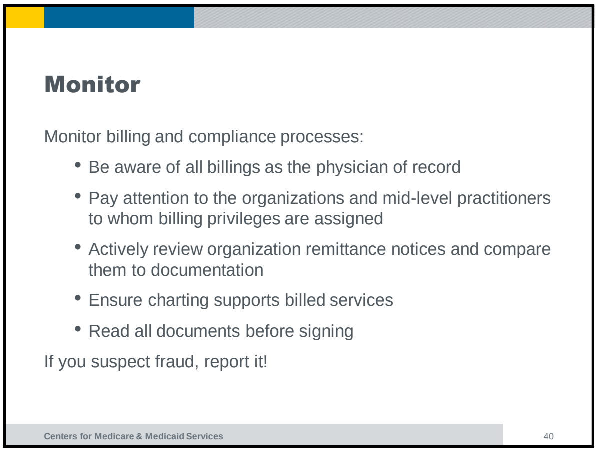
Mitigating Risks

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

Actively Manage Enrollment Information

Actively manage enrollment information with payers by updating:

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

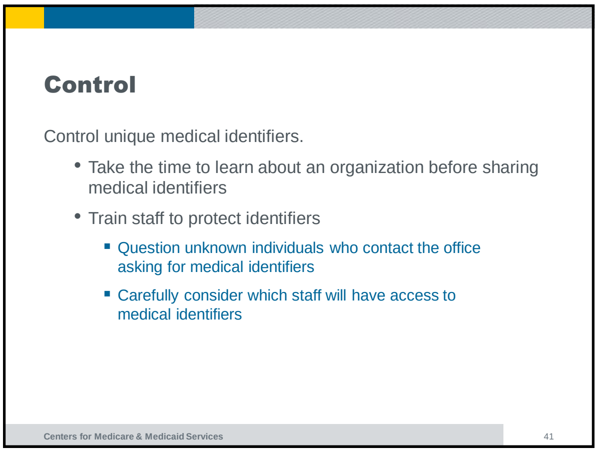


Monitor

Monitor billing and compliance processes:

- Be aware of all billings as the physician of record
- Pay attention to the organizations and mid-level practitioners to whom billing privileges are assigned
- Actively review organization remittance notices and compare them to documentation
- Ensure charting supports billed services
- Read all documents before signing

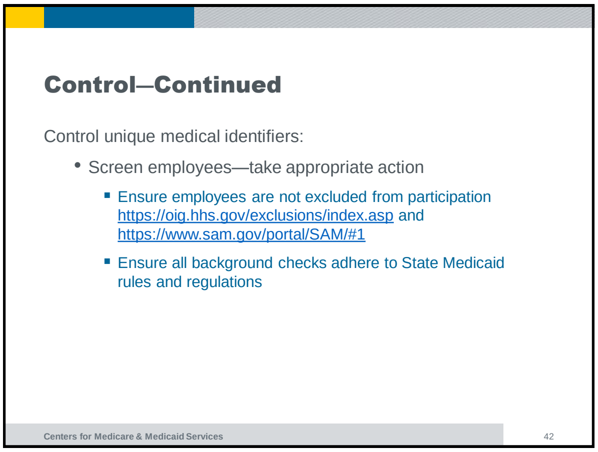
If you suspect fraud, report it!



Control

Control unique medical identifiers.

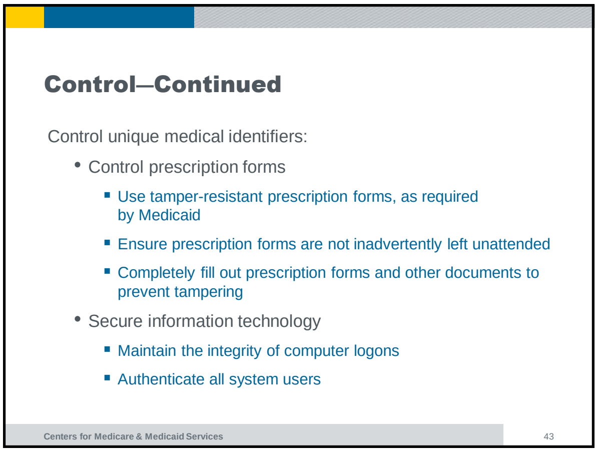
- Take the time to learn about an organization before sharing medical identifiers
- Train staff to protect identifiers
  - Question unknown individuals who contact the office asking for medical identifiers
  - Carefully consider which staff will have access to medical identifiers



Control—Continued

Control unique medical identifiers:

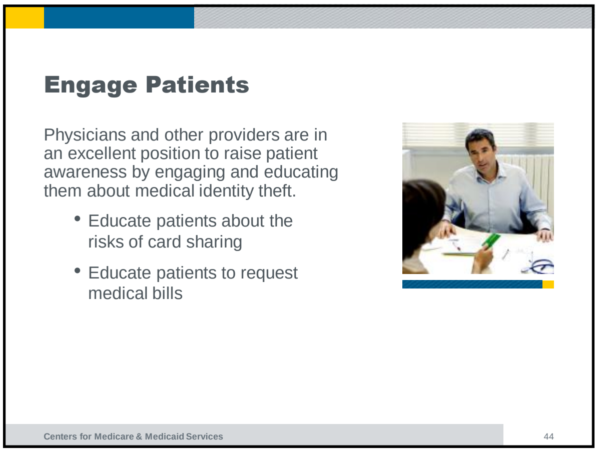
- Screen employees—take appropriate action
  - Ensure employees are not excluded from participation https://oig.hhs.gov/exclusions/index.asp and https://www.sam.gov/portal/SAM/#1
  - Ensure all background checks adhere to State Medicaid rules and regulations



Control—Continued

Control unique medical identifiers:

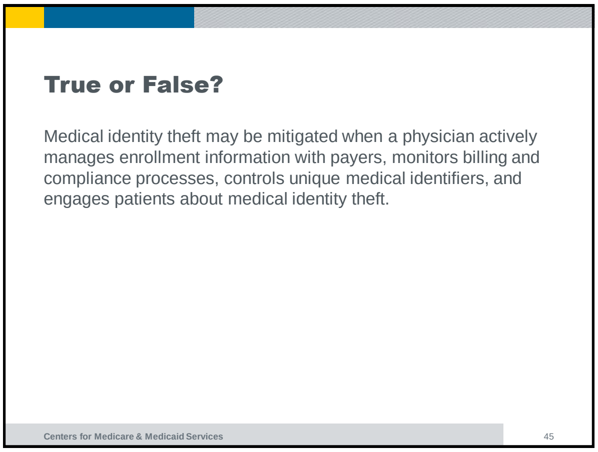
- Control prescription forms
  - Use tamper-resistant prescription forms, as required by Medicaid
  - Ensure prescription forms are not inadvertently left unattended
  - Completely fill out prescription forms and other documents to prevent tampering
- Secure information technology
  - Maintain the integrity of computer logons
  - Authenticate all system users



Engage Patients

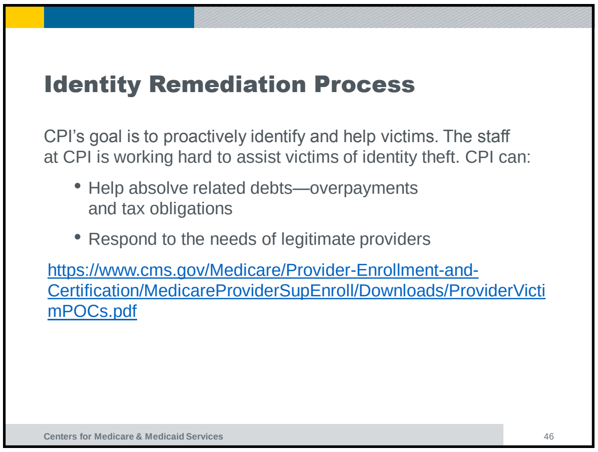
Physicians and other providers are in an excellent position to raise patient awareness by engaging and educating them about medical identity theft.

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



True or False?

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

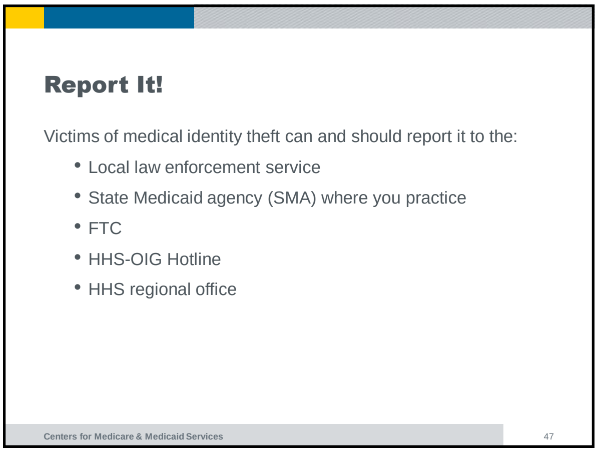


Identity Remediation Process

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

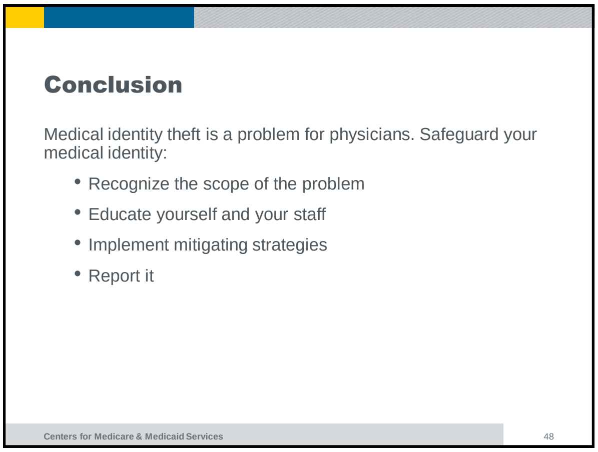
https://www.cms.gov/Medicare/Provider-Enrollment-and-Certification/MedicareProviderSupEnroll/Downloads/ProviderVictimPOCs.pdf



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 Hotline
- HHS regional office



Conclusion

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

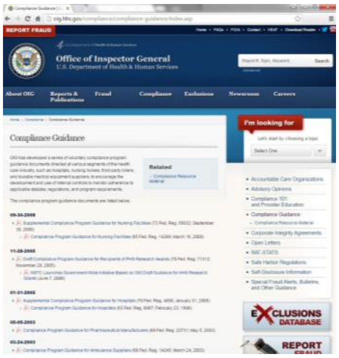
- Recognize the scope of the problem
- Educate yourself and your staff
- Implement mitigating strategies
- Report it

Contacts

- SMA—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
- 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: https://www.consumer.ftc.gov/features/feature-0014-identity-theft
- 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
  Email: HHSTips@oig.hhs.gov
  Website: https://forms.oig.hhs.gov/hotlineoperations/nothhsemployeeen.aspx

HHS-OIG Compliance Guidance

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


oig.hhs.gov/compliance/compliance-guidance/index.asp
REPORT FRAUD
Office of Inspector General
U.S. Department of Health & Human Services
Search
About OIG
Reports & Publications
Fraud
Compliance
Exclusions
Newsroom
Careers
I'm looking for
Let's start by choosing a topic
Select One
Related
Compliance Resource Material
Accountable Care Organizations
Advisory Opinions
Compliance 101 and Provider Education
Compliance Guidance
Compliance Resource Material
Corporate Integrity Agreements
Open Letters
RAT-STATS
Safe Harbor Regulations
Self-Disclosure Information
Special Fraud Alerts, Bulletins, and Other Guidance
EXCLUSIONS DATABASE
REPORT FRAUD

Compliance Guidance

OIG has developed a series of voluntary compliance program guidance documents directed at various segments of the health care industry, such as hospitals, nursing homes, third-party billers and durable medical equipment suppliers, to encourage the development and use of internal controls to monitor adherence to applicable statutes, regulations, and program requirements.

The compliance program guidance documents are listed below.

09-30-2008
- Supplemental Compliance Program Guidance for Nursing Facilities (73 Fed. Reg. 56832; September 30, 2008)
  - Compliance Program Guidance for Nursing Facilities (65 Fed. Reg. 14289; March 16, 2000)

11-28-2005
- Draft Compliance Program Guidance for Recipients of PHS Research Awards (70 Fed. Reg. 71312; November 28, 2005)
  - NSTC Launches Government-Wide Initiative Based on OIG Draft Guidance for HHS Research Grants (June 7, 2006)

01-31-2005
- Supplemental Compliance Program Guidance for Hospitals (70 Fed. Reg. 4858; January 31, 2005)
  - Compliance Program Guidance for Hospitals (63 Fed. Reg. 8987; February 23, 1998)

05-05-2003
- Compliance Program Guidance for Pharmaceutical Manufacturers (68 Fed. Reg. 23731; May 5, 2003)

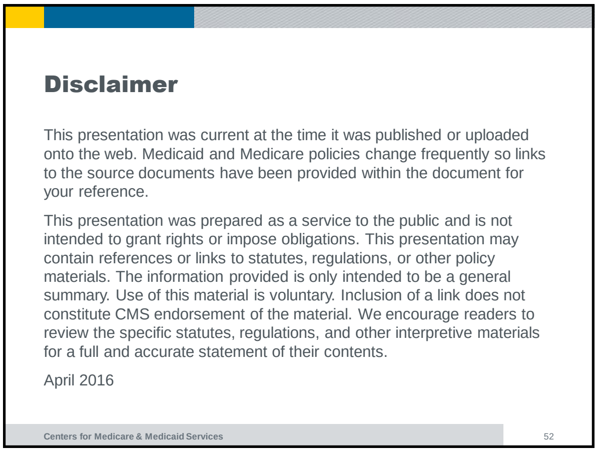
03-24-2003
- Compliance Program Guidance for Ambulance Suppliers (68 Fed. Reg. 14245; March 24, 2003)

Questions

Please direct questions or requests to: MedicaidProviderEducation@cms.hhs.gov

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

Follow us on Twitter #MedicaidIntegrity



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.

April 2016

Centers for Medicare & Medicaid Services 52