MEDICAL IDENTITY FRAUD ALLIANCE

Medical ID Theft & Fraud

Ann Patterson

Senior Vice President, Program Director

Medical Identity Theft Primer

- Includes theft of Protected Health Information (PHI) and/or Personally Identifiable Information (PII) for the purpose of financial gain or to unlawfully obtain medical goods or services
- Victims include the patient, healthcare providers, insurance companies, taxpayers and consumers who subsequently pay higher prices for their care
- Contributing factors
  - Pervasiveness of electronic PHI
  - Significant increase in the value of PHI because of its use by hackers and criminal organizations
  - Increasing number of individuals with healthcare benefits
  - Increasing alternative delivery models that include care outside of facilities
  - Lack of coordinated response by public and private sectors to protect the privacy and security of PHI
- Changing legal and regulatory landscape – as law keeps pace with technology, there will be additional regulations and increasing penalties for noncompliance

Some Facts

- Fraud adds $80 billion in excess costs to health care annually 1
- $41.3 billion per annum estimated economic impact 2
- 30+ million medical records have been disclosed since 2009 3
- 1 in 4 chance of being a victim of ID fraud as a result of data breach 4
- Only 15% of insured adults familiar with medical identity theft 5
- The average per record cost of a data breach for U.S. organizations is $188 6
- Growth in Electronic Health Records (EHR) and the new health insurance exchanges may magnify the problem
- Stolen, ransomed or misused patient data is at the core of many crimes perpetrated by the gamut of fraudsters, including organized crime

[1] 2012 National Academy of Sciences Health Care Study
[2] 2013 Javelin Strategy & Research Identity Fraud Report
[3] http://www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/breachtool.html
[4] https://www.javelinstrategy.com/blog/2013/04/28 financial-pain-ensues-when-custodians-of-health- fail-to-be-good-stewards-of-privacy/
[5] 2012 Harris Interactive/Nationwide Study: Few Aware of Risk of Medical Identity Theft
[6] 2013 Ponemon Institute Research Report: 2013 Cost of Data Breach Study – Global Analysis

Types of Medical ID Fraud

- Obtain healthcare services or treatment
- Obtain Rx or medical equipment
- Obtain Medicare, Medicaid or other government benefits
- Healthcare records were accessed or modified
- Credit report was accessed or modified
- Obtain fraudulent credit accounts

Impact on Victims

- 64% did not incur any out-of-pocket costs
- 36% paid an average of $18,660
- 73% suffered other types of financial consequences; e.g., diminished credit score or financial ID theft
- Resolution of the crime is time-consuming
  - 36% of respondents report it took a year or more to resolve the problems
- Misdiagnosis, mistreatment or delay in treatment

Financial Impact

- Reimbursements to healthcare provider to pay for services provided to imposter/identity thief
- Identity protection, credit reporting, legal counseling
- Costs for medical care or services due to lapse in healthcare coverage
- Out-of-pocket payments to health plan
- Increase in insurance premiums

Non-Medical Consequences

- Lost time and productivity fixing inaccuracies in records
- Diminished credit score
- Financial ID theft
- Legal fees
- Employment related difficulties
- Revocation of licenses

Medical-related Consequences

- Lost trust/confidence in healthcare provider
- Misdiagnosis
- Delay in receiving care
- Mistreatment
- Incorrect medication prescribed
- Loss of health insurance

Lacking Awareness

- Individuals lack awareness of the seriousness of the crime
- 50% do not take any steps to protect themselves from medical identity theft
- 50% not aware medical identity theft can create inaccuracies in their permanent medical records

Education Needed

- 56% do not check their medical records for accuracy
  - Don’t know how
  - They trust their providers to be accurate
  - Do not think to check
  - Records not easily accessible
  - Don’t care
- 54% do not review their EOBs
  - Trust accuracy
  - Do not understand
  - Not important

Preventable Fraud

- Sharing of personal identification for medical services is prevalent
- 58% shared their personal identification or medical credentials with someone they knew
  - 30% knowingly shared
  - 28% family member took identification or medical credentials without consent

Industry Costs

- 8200 out of every 1 million Americans will be a victim or, or complicit in, medical identity fraud
- 58% of cases involved sharing medical ID with an acquaintance (4760 out of 8200)
- $7,598 estimated average annual per capita cost for health care in the US (Kaiser Family Foundation)*
- The cost of health care to “false identities” is approximately $36M (4760 x $7,598) for every 1M insured individuals
- Medical identity fraud is generally not reported – the actual costs may be higher

For More Information

Ann Patterson
Senior Vice President and Program Director
703-407-0958
Ann@MedIDFraud.org

http://medidfraud.org