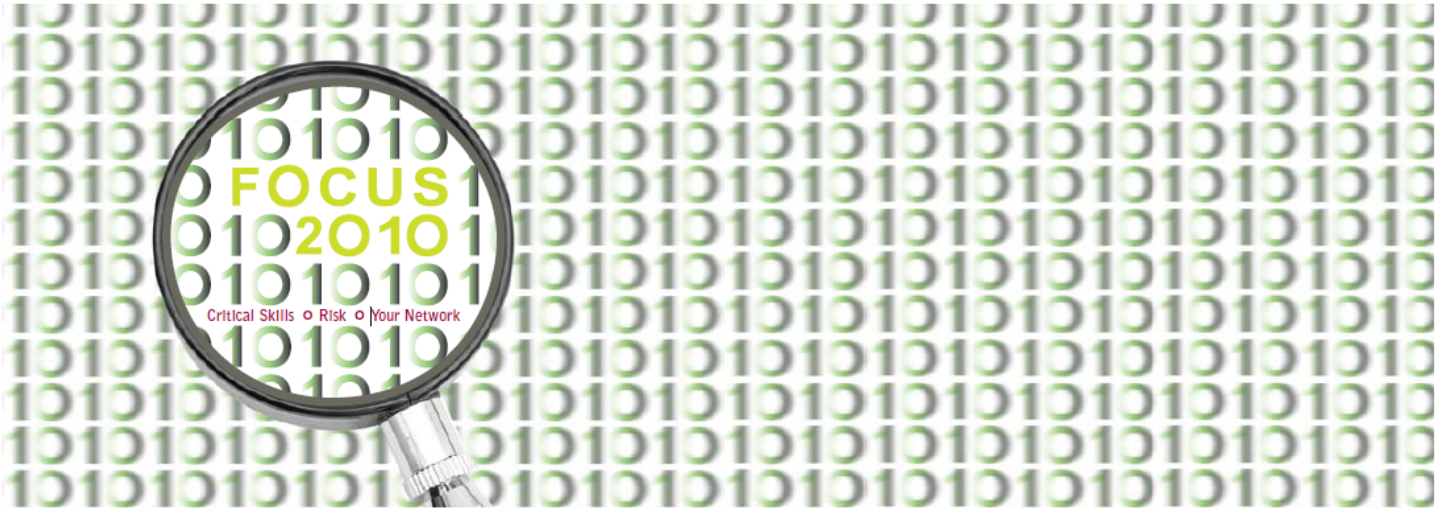
10th Annual SF ISACA Fall Conference

October 4 – 6, 2010



S12: Medical Identity Theft and Red Flag Rules: The Health Plan Perspective

Marita Janiga, Kaiser Permanente

ISACA®

Trust in, and value from, information systems

San Francisco Chapter

ISACA
Trust in, and value from, information systems
San Francisco Chapter

Medical Identity Theft and Red Flag Rules: The Health Plan Perspective

KAISER PERMANENTE®

Marita C. Janiga
Director, National Special Investigations
National Compliance, Ethics & Integrity Office
Kaiser Foundation Health Plan

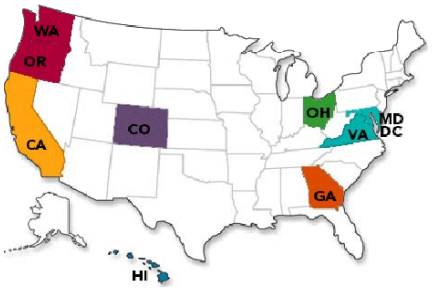
What We Will Cover

- About Kaiser Permanente
- What Is Medical Identity Theft
- "Red Flag" Regulations
- How Kaiser Permanente Is Proactive
- Data Mining for Identity Theft
- Case Studies from Our Investigations

ISACA
San Francisco Chapter

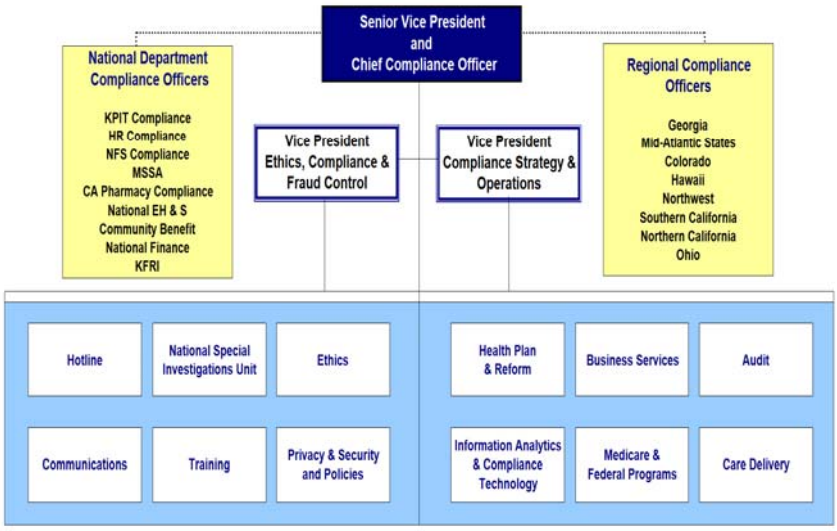
About Kaiser Permanente

- Nation's largest nonprofit health plan
- Integrated health care delivery system
- Over 15,000 physicians
- Over 164,000 employees
- Serving 9 states and the District of Columbia
- 35 hospitals and medical centers
- 454 medical offices
- $42.1 billion annual revenues



(as of December 31, 2009)

National Compliance, Ethics & Integrity Office



Kaiser Permanente Members Are Connected

As of December 31, 2009 …

- Kaiser Permanente members have the benefit of Kaiser Permanente HealthConnect, our electronic medical record system
- 3 million active users of “My Health Manager” on KP.org
- 1.8 million lab results online monthly
- 150,000 appointments scheduled online each month
- Over 700,000 e-mails monthly
- 550,000 prescriptions filled online monthly
- More than 300,000 parent/guardians registered to use “Act for a Family Member”

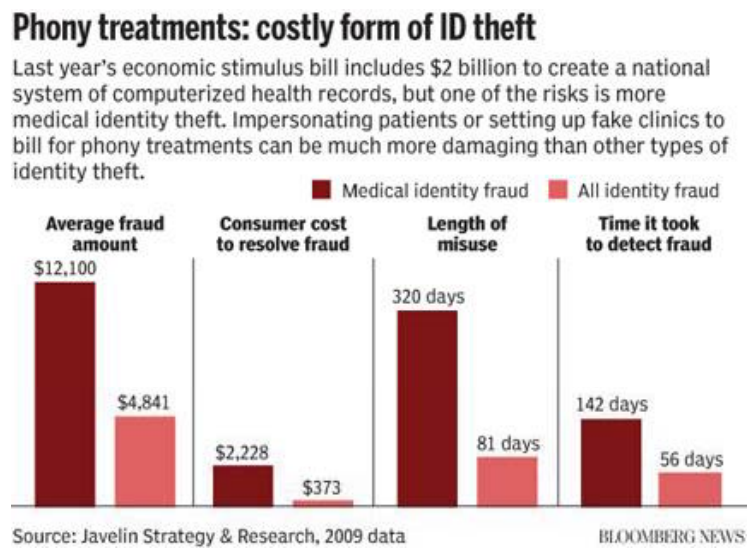
Medical Identity Theft

- Medical identity theft occurs when a patient’s identity is used by someone else to get health care
  - Medical identity theft can be voluntary – such as card sharing between family or friends
  - Medical identity theft can be involuntary – such as when someone’s wallet is stolen or patient data is sold to bogus vendors who falsely bill the government

Potential Consequences of Medical ID Theft

- Compromised medical records that could create patient safety issues
- False medical/pharmaceutical billings/claims
- Denial of health insurance claims
- Denial of health insurance coverage
- Denial of life insurance claims
- Denial of life insurance coverage
- Denial of employment based on false medical history
- Time and expense correcting false patient/insurance records

The Cost of ID Theft



Increasing Media Coverage

Bipartisan Medicare Fraud Enforcement and Prevention Act (MFEPA) of 2010

Enhanced Criminal Penalties

- MFEPA will double the criminal penalties for making false statements in connection with services that are paid for, in whole or in part, by a Federal Health Care Program, and for violating the anti-kickback statute from 5 years to 10 years of imprisonment and increase fines from $25,000 to $50,000
- MFEPA will also create a new offense for illegally distributing a Medicare or Medicaid beneficiary ID or billing privileges and will establish a maximum penalty of 3 years in prison and a fine

Bipartisan Medicare Fraud Enforcement and Prevention Act (MFEPA) of 2010 *cont.*

Medicare Fraud Prevention

- Implements criminal background checks, finger-printing, and random site visits for high-risk suppliers and providers to ensure they are legitimate businesses before they cash a single Medicare check.
- Directs Secretary of Health and Human Services (HHS) to provide law enforcement officials with real-time access to data necessary for combating Medicare fraud.
- Directs Secretary of HHS to conduct a pilot program that implements biometric technology to ensure that Medicare beneficiaries are physically present to receive certain services covered under Medicare.

Bipartisan Medicare Fraud Enforcement and Prevention Act (MFEPA) of 2010 *cont.*

Oversight of Medicare Contractors

- Directs Government Accountability Office to study Medicare contractors, including Recovery Audit Contractors, and report back to Congress with recommendations for legislation and administrative action.

New Red Flag Regulations

- Authority – Part 681 of Title 16 of the Code of Federal Regulations implementing Sections 114 and 315 of Fair and Accurate Credit Transactions Act (FACTA) of 2003
- Program Requirements for ID Theft
  - Identify Red Flags
  - Detect Red Flags
  - Respond to Red Flags
  - Updates to Program (oversight and review)
  - Board Approved

FTC Red Flags Regulation – How We Prepared

- On May 1, 2009, the National Compliance, Ethics and Integrity Office established an Identity Theft Prevention Program designed to:
  - Identify and detect relevant Red Flags for covered accounts Kaiser Permanente offers or maintains, and incorporate these Red Flags into the Program
  - Respond appropriately to any Red Flags that are detected to prevent and mitigate identity theft
  - Ensure the Program is updated periodically to reflect changes in risks to customers

FTC Red Flags Regulation – How We Prepared *cont.*

- The National Compliance Office was been designated by the Boards of Directors to develop, implement, oversee and administer the Identity Theft Prevention Program
- This program is designed to comply with the FTC Red Flags Rule which will likely be implemented sometime in the future

(FTC Red Flags Rule implementation date is TBD)

Red Flags for Identity Theft

- Red Flags are defined as “a pattern, practice, or specific activity that could indicate identity theft”
- The FTC identifies these examples of Red Flags for ID theft:
  - Suspicious documents and/or personal identifying information, such as an inconsistent address or nonexistent Social Security number
  - Unusual use of or suspicious activity relating to a patient account
  - Notices of possible identity theft from patients, victims of identity theft or law enforcement authorities
  - Alerts, notifications or warnings from a consumer reporting agency

How Kaiser Permanente Is Proactive

- Established a National ID Theft Prevention Policy
- Check photo ID when patient appears for care – developed a “Check ID Toolkit”
- Effective Compliance Program and Hotline
- Excellent Forensic IT Tools
- Liaison with law enforcement
- Communicate what happens to perpetrators (terminated and prosecuted)
- Engage in targeted proactive data mining

Proactive Data Mining for Identity Theft

- Services After Death (SAD)
- Birth with no pre-natal or post-natal care
- Medical services out of scope (male patient in OB/Gyn)
- Dramatic changes in height / weight with no medical indicators
- Suspect SSN use
- Drug seeking behaviors

We Are a Health Care Company

- Our frontline staff and care providers have been given tools and protocols to follow when they suspect medical identity theft
- We provide care if someone in need comes to one of our facilities, even if we suspect identity theft

Photo ID Protocol

Best, Primary Photo Identification:

- Government issued driver's license or state identification card
- Military identification card
- Government issued passport or residency card

Acceptable, Secondary Photo Identification:

- School ID card with photo
- Employee ID card with photo
- Financial institution ID with photo (bank card)

If No Photo Identification:

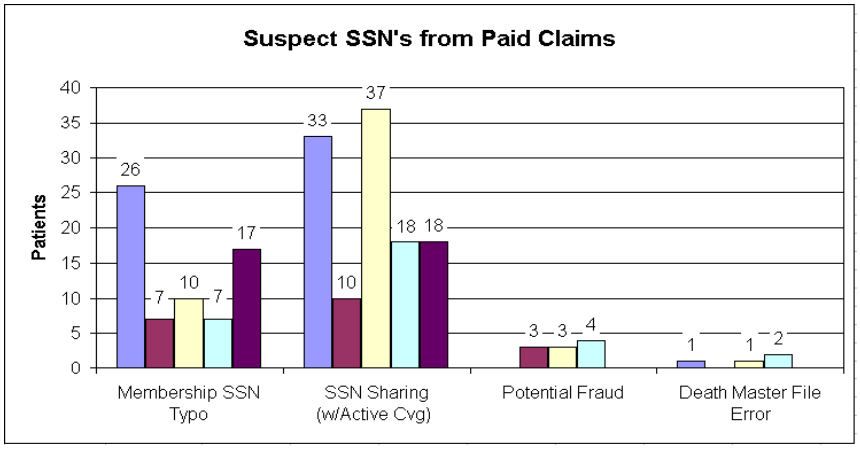
Patient must provide at least (3) unique identifiers (patient demographics)

- Address
- Phone Number
- Last (4) digits of Social Security Number
- Birth date
- Subscriber name on health plan

When there is a concern/suspicion that the individual presenting is not the actual patient (after attempting to match three patient demographic identifiers in addition to patient's full name):

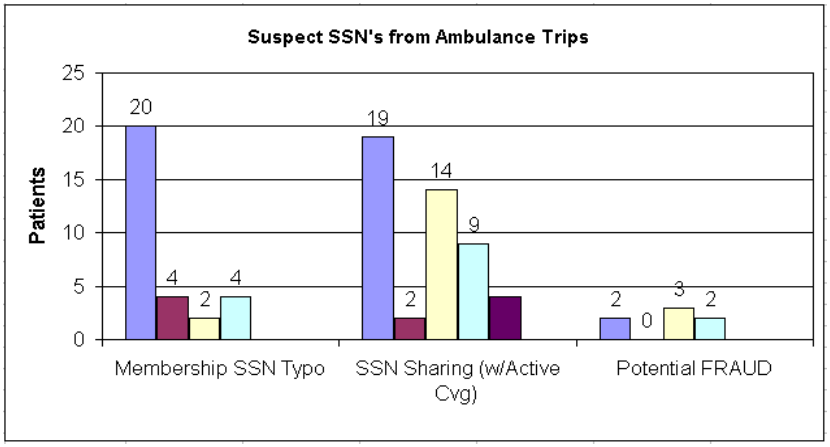
- For urgent medical services, allow patient to be seen.
  - References: EMTALA 42 USC Sec. 139dd;
  - KP Policy #: NATL.REVCYC.011

Data Mining Findings



Review of 4.5mm claims for 2+mm members surfaced the information. SSN sharing and potential fraud are under review by NSIU.

Data Mining Findings



Review of 1 years ambulance data for 2+mm members surfaced the above information. SSN sharing and potential fraud are under review by NSIU.

How Kaiser Permanente is Reactive:
National Special Investigations Unit (NSIU)

- Ten investigators with strong law enforcement backgrounds
- Experienced in criminal and fraud investigations
- Responsible for conducting internal investigations
- Supported by Fraud Analysts with strong operational backgrounds

NSIU Collaborates With …

- Information Analytics and Compliance Technology (iACT) Team (data mining)
- Information Technology Forensics (computer forensics)
- Regional and Local Privacy and Security (many cases have a potential HIPAA concern)

Case Study – Card Sharing

- Patient admitted to hospital and surgery was performed
  - Member had allowed sick friend to use his/her identity for care
- Copy of government identification and timekeeping records obtained from employer
  - Timekeeping records revealed member was at work during hospitalization
- Friend presented for medical exam and was photographed
  - Photo did not match member
- Case referred to Law Enforcement
  - Member pled guilty to criminal charges
  - Ordered to pay restitution

Case Study – Card Sharing

- Member allowed a friend who is having headaches to use his Kaiser Permanente card to see a doctor
- Physician orders a CT scan that indicates brain surgery is necessary
- Friend is admitted and brain surgery is performed
- Months later, when the member seeks treatment, the primary care physician is amazed at the quick recovery
- Member admits to the physician that it was his friend who had the surgery

Case Study – Unwitting Member

- Former member received a bill and believed his ex-wife was letting her boyfriend use his identity for care
- NSIU coordinated with Law Enforcement
- Law Enforcement confronted the ex-wife and boyfriend with the evidence and they admitted to the identity theft
- Law enforcement pursued criminal prosecution

Drug Seeking – Multiple Cases

- Non-member presents at the Emergency Department using a false identity to obtain controlled substances
- The individual reports he/she is in pain, often claiming a work-related injury
- The individual files a workers' compensation claim and is treated for what is believed to be a work injury
- The claim turns out to be false – no such company exists or the individual filing the claim does not work there
- The individual repeats this routine at multiple emergency departments throughout the area, at both Kaiser Permanente and non-Kaiser Permanente facilities

Take Aways

- A clearer understanding of what Medical Identity Theft is
- How Medical Identity theft affects patients, the health care industry and the economy at large
- The impact of the Red Flag rules on the health care industry
- How KP works to protect its members from medical identity theft

Questions?

Marita Janiga
Marita.C.Janiga@kp.org
(510) 271-6937
Kaiser Permanente
Director, National Special Investigations Unit
National Compliance, Ethics, and Integrity Office