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

Session Number - P11
Medical ID Fraud

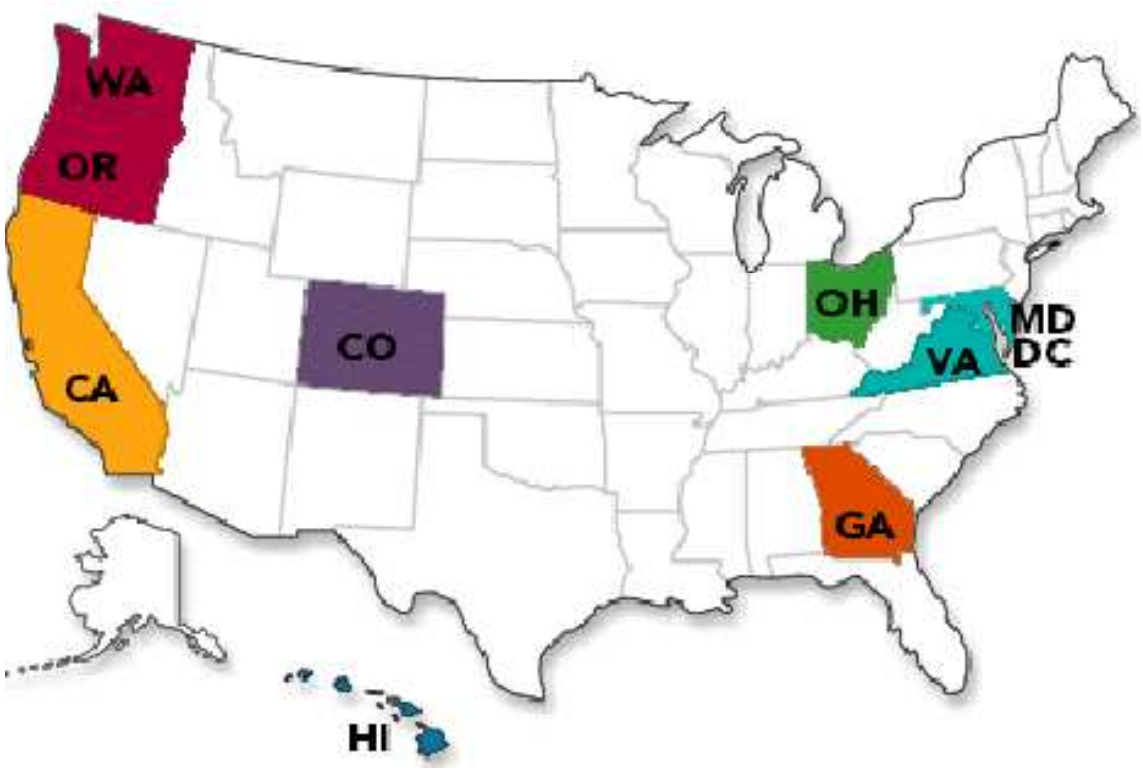
Electronic Medical Record – Risk Landscape

Objectives

- Learn how to investigate allegations of medical identity fraud
- Learn how to prevent and identify potential medical identity fraud through analytical data mining
- Learn medical identity fraud definitions and recognize the regulatory environment for medical identity fraud, related HIPAA violations
- Learn how Kaiser Permanente protects its members from medical identity fraud through proactive data mining and analysis

About Kaiser Permanente

Founded in 1945, Kaiser Permanente is one of the nation's largest nonprofit health plans, serving more than 8.7 million members, with headquarters in Oakland, California.



By the numbers

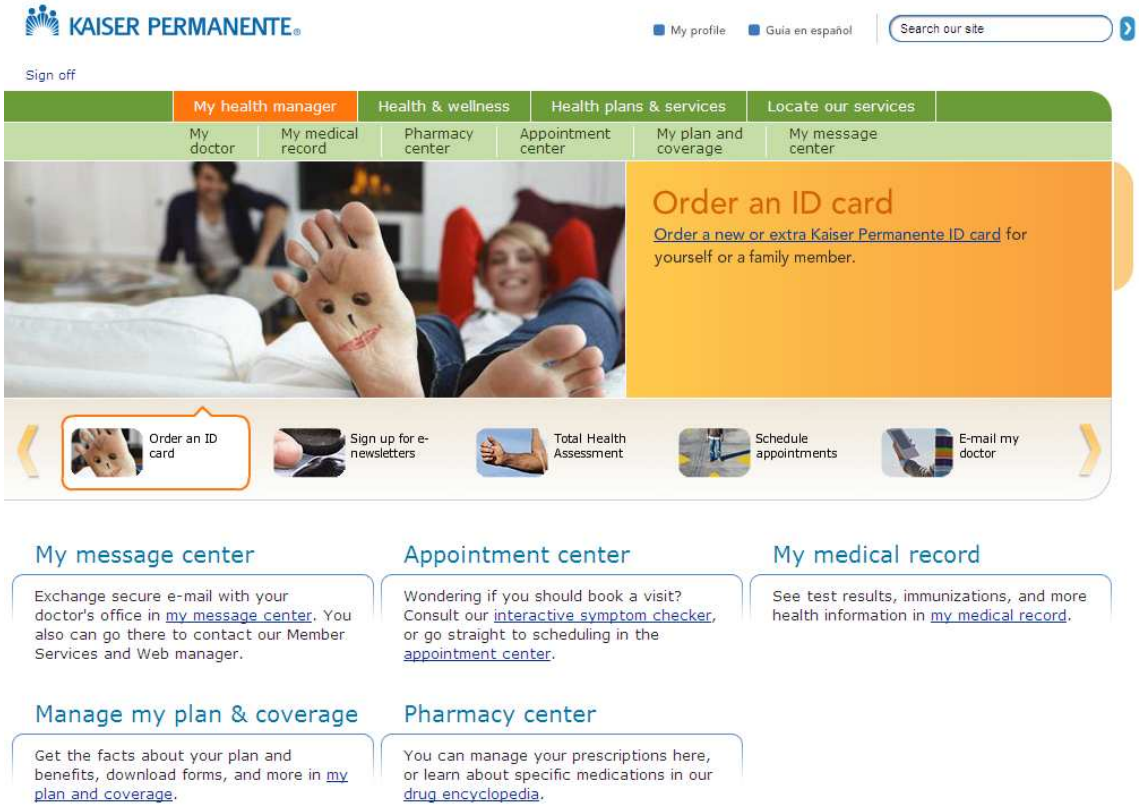
Total membership	**8.7 Million**
Hospitals	35
Medical offices	454
Physicians Approximate, representing all specialties	15,129
Employees Approximate, representing technical, administrative, and clerical employees and caregivers (includes 45,270 nurses)	164,098
Doctor office visits (annually)	36.6 Million
Prescriptions filled (annually)	132.2 Million
Number of outpatient pharmacies	383

Industry-leading personal health record

KP HealthConnect is an electronic health record (EHR), linking our 8.7 million members securely to their health care teams, personal health data, and the latest medical knowledge

My Health Manager on kp.org

- Kaiser Permanente HealthConnect® is the combination of our EMR and PHR (My Health Manager)
- In March 2010, every medical facility within the health system was equipped with KP HealthConnect®



HealthConnect® by the numbers

Members using My Health Manager	3 Million
Secure e-mails (Sent to physicians and clinicians)	8.6 Million
Lab test results view online	21.7 Million
Online requests for appointments	1.8 Million

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

Back to Business

2008 Highlights

- 47 million visits to kp.org, averaging about 130,000 visits per day
- More than 933,500 members became new registered users
- More than 16 million lab test results viewed online

My Health Manager's secure features – by the numbers

- 6,078,838 e-mails between caregivers and members
- 16,773,273 test results viewed
- 5,661,660 online prescription refills
- 1,403,870 appointment requests
- 38,260,038 sign-ons

Kaiser Permanente Internet Metrics, 2008 Annual Report, Kaiser Permanente Internet Services Group, February 2009

Risk landscape

- Lost and stolen ePHI
  - Unencrypted devices of all types
  - Unintended disclosures
- Inappropriate access to PHI
- Health Information Exchanges (HIE) becoming more prevalent
- Greater fines and penalties

Medical Identity Fraud

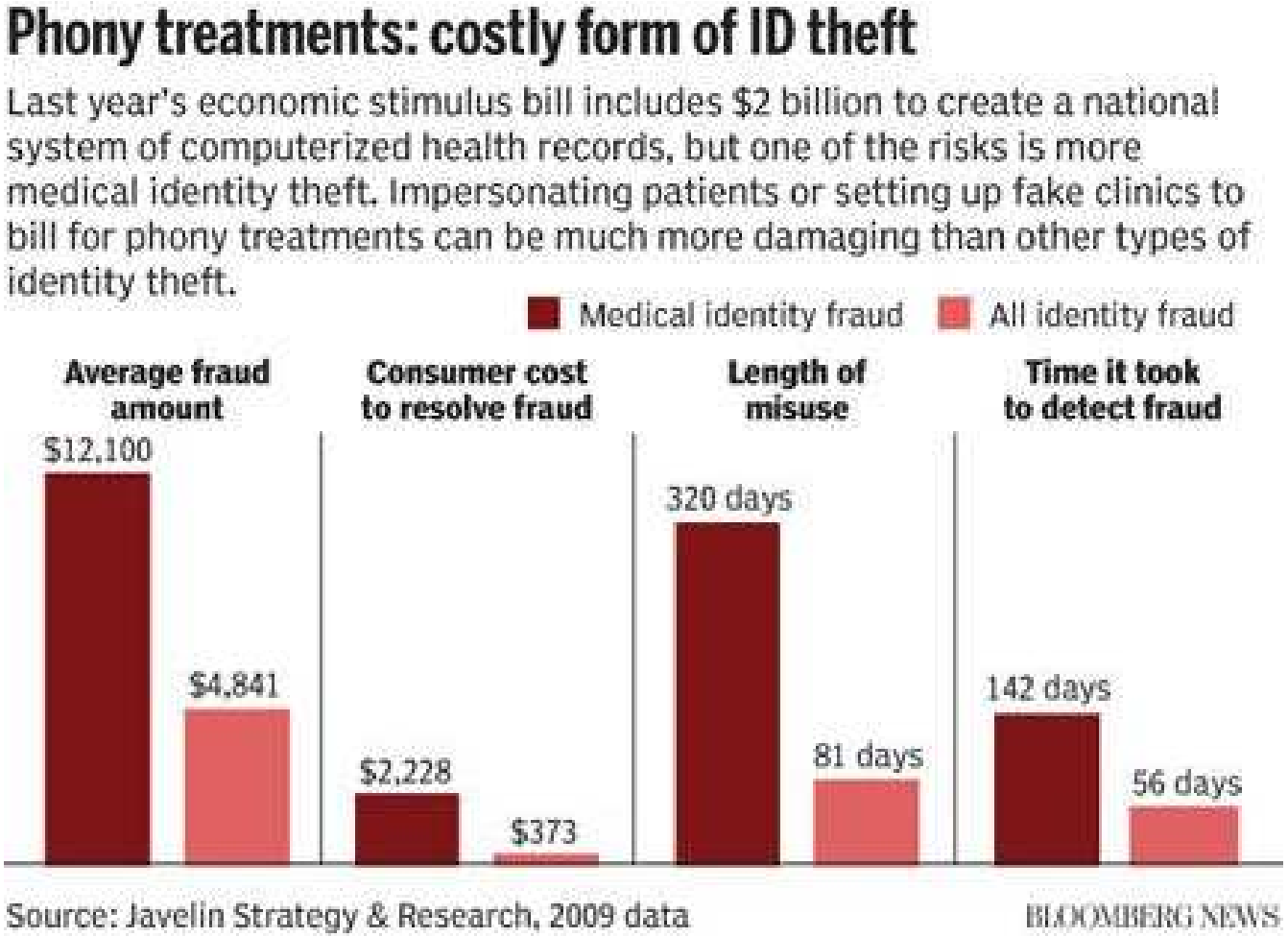
- Medical identity fraud occurs when a patient's identity is used by someone else to get health care
  - An individual may be complicit in medical identity fraud by sharing his/her medical card with family or friends

    OR
  - Medical identity fraud can occur through other means 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 Fraud

- 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



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

Additional Regulations impacting Health Care

- American Recovery and Reinvestment Act (ARRA) of 2009 Title XIII-Health Information Technology for Clinical Health (HITECH)
- ARRA represents the largest change in privacy and information security requirements since the 2003 and 2005 Health Insurance Portability and Accountability Act (HIPAA).
  - New patient privacy rights
  - Regulations for business associates
  - Breach reporting requirements
  - Increased enforcement and penalties

External Reporting Requirements

- CMS Annual Part D Fraud, Waste, and Abuse Report
- CalPERS Kaiser Permanente National Fraud Control Annual Report
- Federal Employee Health Benefit Plan/Office of Personnel Management National Fraud Control Annual Report
- California Dept of Managed Health Care Anti-fraud Report, Kaiser Foundation Health Plan, Inc., California Regions
- California Department of Insurance
- Maryland and District of Columbia Departments of Insurance

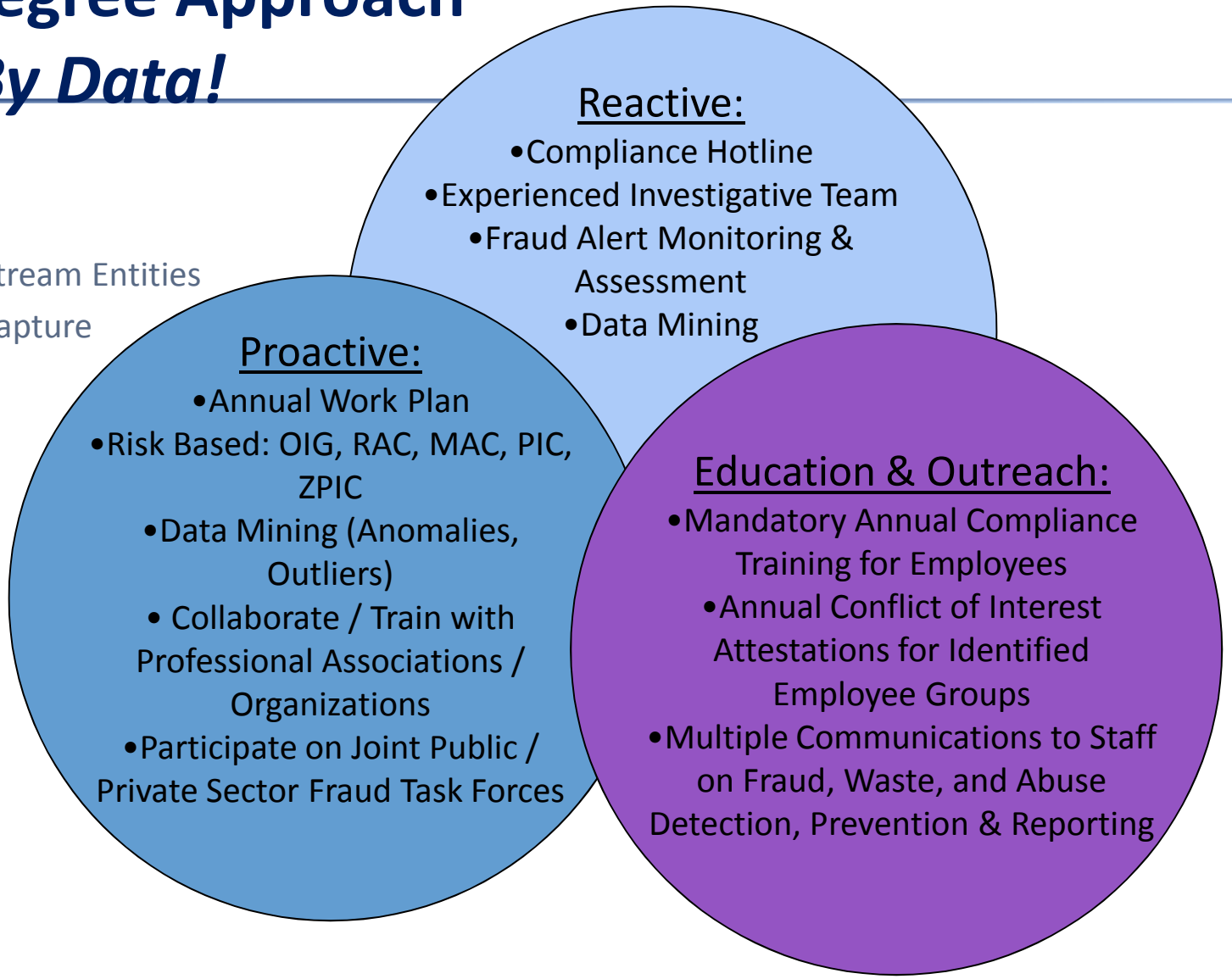
Changing Enforcement Environment

- In 2010, the Centers for Medicare and Medicaid Services (CMS) expanded its focus on enforcement through auditing and data mining to identify potential false claims.
- An industry wide doubling of False Claim Act denials and recoveries has been forecasted.
- CMS plans to expand audits in Medicare Advantage and Medicaid programs.

A 360-Degree Approach
Driven By Data!

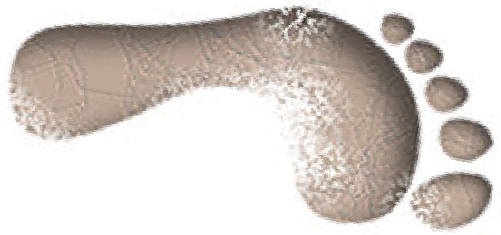
Hot Topics:

- Identity theft
- First Tier Downstream Entities
- Complete care capture
- PBM Oversight



Data Approach: Our Data Footprint

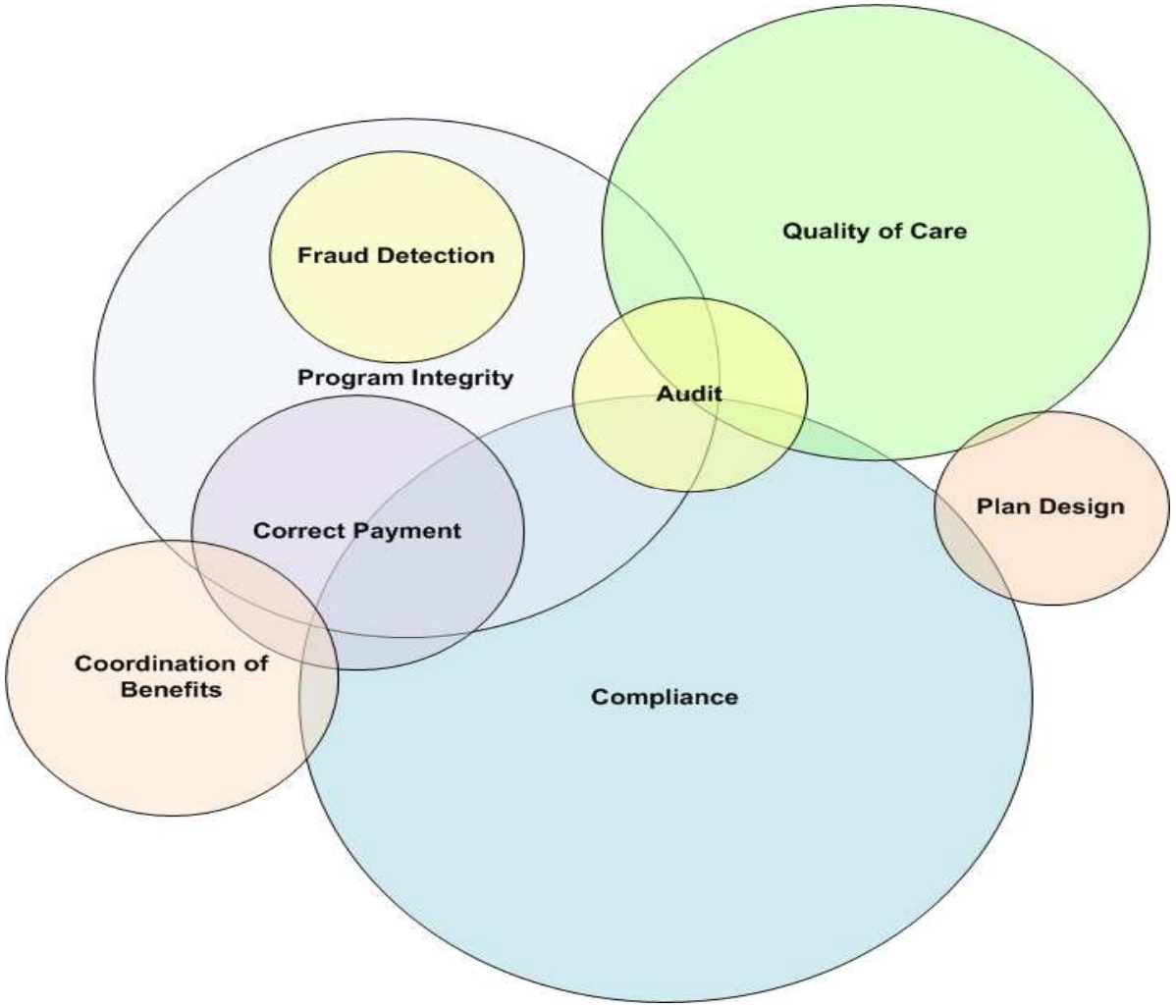
- **Counts and Amounts:**
  - Over 60 terabytes of non-encounter data
  - 8 categories with 69 active data sources
  - 5,605 tables (12% increase)
  - 143,243 columns (8.5% increase)
  - 18.8 billion records (10% increase)
- **Data is refreshed:**
  - Daily 4 sources
  - Bi-weekly 14 sources
  - Monthly 44 sources
  - Quarterly 6 sources
  - On-demand 3 sources
- **Encounter data:**
  - > 900 terabytes
  - All encompassing: Physician notes, Laboratory, Radiology, Pharmacy orders, etc



- **Pharmacy data:**
  - > 1.2 petabytes
  - All Rx's up to 15 years
  - Utilization & pricing data

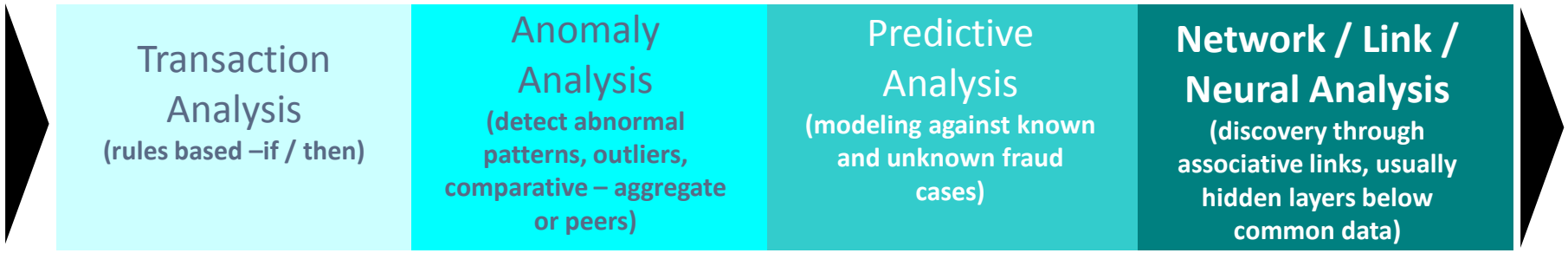
Approximately 75% of Fraud, Waste, and Abuse Data Also Supports our "Program Integrity" Efforts

Our Data Mining program runs over 1.2 million queries per year



Data Mining Analytics Continuum

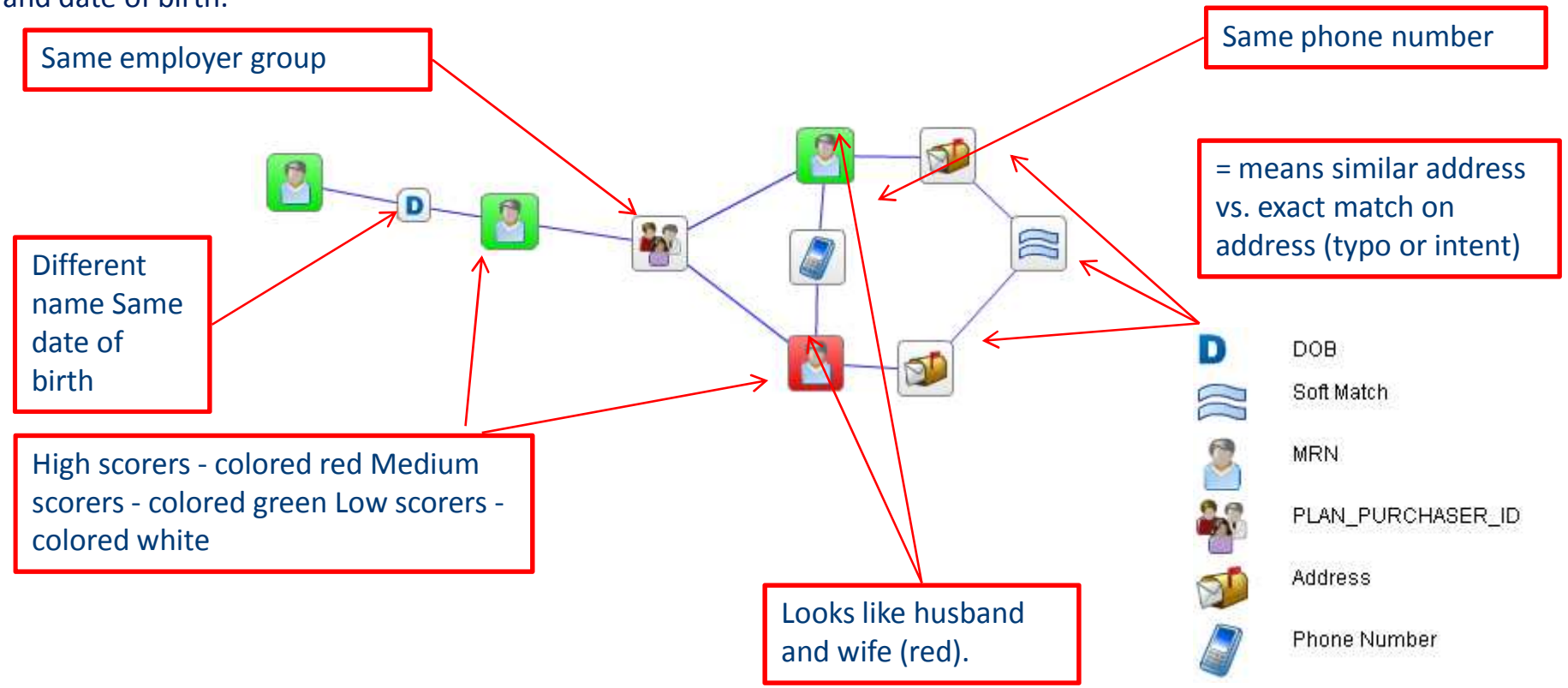
Common Technology → **Advanced Technology**



Data Analytics: Link / Network Analysis

How to interpret a network diagram:

The goal of Link Analysis (also known as social or network analysis) is to uncover potential member fraud networks by linking flagged members based on name, address, home phone number, employer (plan purchaser), and date of birth.

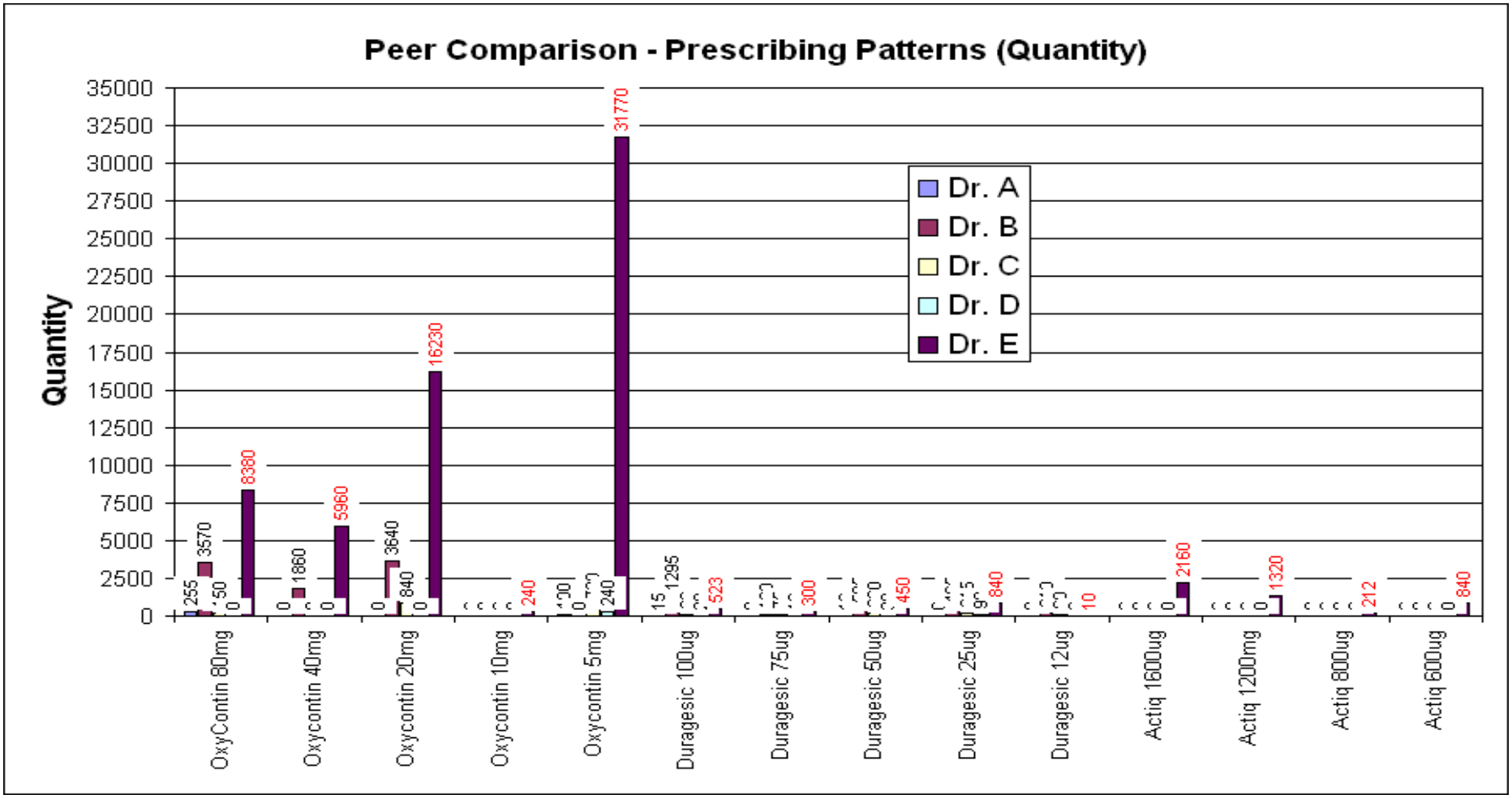


Algorithm Design & Creation: DSB Scoring Grid

Purpose	Variable	Max Points
1. Fake identity/false Rx	Non-member or member inactive	10
2. False Rx	Percent of new Rx with no doctor visit 50% = 8, 25%=5, 10-24%=3	10
3. Multiple sources	Number of KP pharmacies > 5=10pts, 3=5pts	10
4. Multiple sources	Number of prescribers 5=10pts, 3=7pts	10
5. Drug user	Number of other fraud prone drugs 5=10pts, 4=8pts, 3=6pts	10
6. Existing medical condition	Number of doctor visits not involving this drug 0 gets 10pts, 6+ gets 0pts	10
7. Desperation	Distance traveled vs. non-fraud prone scripts 20miles=10pts, 15=7pts	10
8. Heavy usage	12-month total quantity w/o cancer diagnosis and w/o PM specialist… Metric is Drug / time period dependent	10
9. Escalating usage	Slope of dose per day upward = 10, flat =5	10
10. Prolonged usage	Number of months with purchase w/o cancer diagnosis and w/o PM specialist 10 months or more=10pts, 6-9=5pts	10

Prescribing Patterns / Script Mills

Case #1

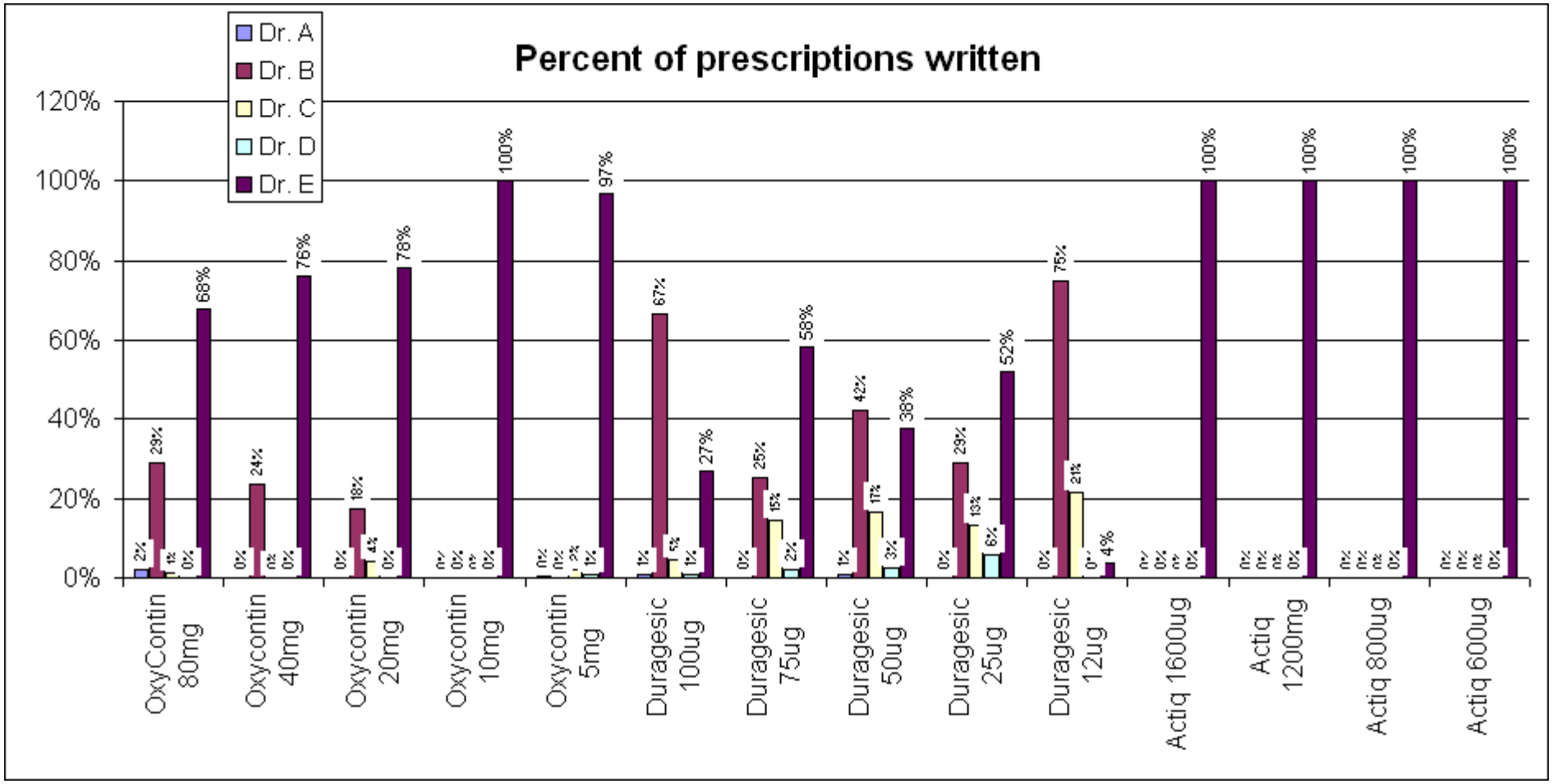


ISACA
Trust in, and value from, information systems
San Francisco Chapter

Back to Business

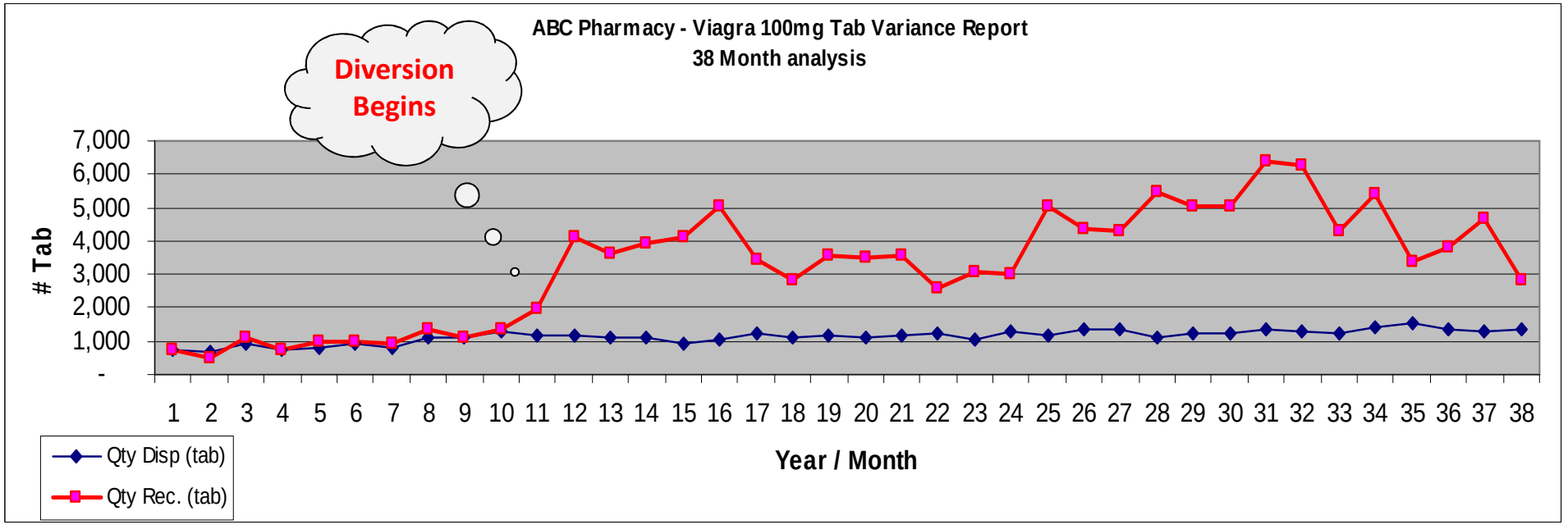
Prescribing Patterns / Script Mills

Case #1



Inventory Control – aka In / Out Studies

Case #2



Data Mining for Comprehensive Application Access Monitoring

System Access type algorithms in use:

- User accesses adult medical records from a pediatric position
- User accesses male records from an OB-GYN position (not part of fertility treatment)
- User accesses medical records shortly after patient checks out for no medical reason
- User accesses records of patients with same name as they have
- User accesses records of patients never cared for at their clinic or hospital
- User accesses demographics of records when that is not part of their job (e.g. phlebotomist does not need to know where patient lives)

Monitoring HIPAA compliance and identity theft

- User prints a very high number of medical records for position assignment
- User views medical record numbers sequentially and this is not part of the position or assignment
- User changes elements in a medical record that do not change (e.g., blood type, date of birth)
- User accesses records when there is no corresponding medical visit
- User accesses records of patients who are no longer health plan members

Investigating the allegations

Internal

- Credit fraud through identity theft
- Real estate fraud through identity theft

External

- HIPAA breach by former spouse

Contact Information

Marita Janiga

National Compliance, Ethics, and Integrity Office

Director of National Special Investigations Unit

510.271.6937

marita.c.janiga@kp.org

Jay Loden

National Compliance, Ethics & Integrity Office

Information Analytics and Compliance Technology Department / Data Analytics

626.674.4476

jay.m.loden@kp.org