CompassCare

HIPAA:

Where Atomic Data Collides With Distributed DNA

Or, why health data and people will always be a problem and what can be done to improve it

June 26th, 2005

Health Information Usage & Issues

- Public sector/ Community Health:
  - Government- local, state, federal
  - University R&D
- Private sector/ Commercial Health Info:
  - Patients
  - Providers
  - Employers/ Payers
  - Drugs/ Devices
- Technology, Design, Management:
  - Secure system design
  - Secure operating systems and databases
- The Real Problem => “adoption & the inside job”

Public Sector/ Community Health Data Drivers

- Local, State, Federal Governments:
  - More rapid and comprehensive identification of public health issues related to bio-hazards and chronic disease
  - Identification of homeland security issues e.g. bio-terrorism outbreaks of anthrax, small pox, etc.
- Universities and R&D:
  - Need for better, more rapid and comprehensive data related to biotech and disease research
  - Identify better potential populations for R&D purposes whether those requirements need diversity or homogeneity.

Private Sector/ Commercial Health Data Drivers

- Patients:
  - Want better and safer patient care
  - Need ability to maintain data
  - Need ability to authorize access to “my health info”
- Providers:
  - Goal is better care for their patients
  - If too efficient, potential loss of revenue (less visits, less labs)
  - Lots of data is better clinically, but Catch 22 is efficiency
  - “Ownership” of data is competitive advantage
- Employers/ Payers:
  - Want healthy, productive employees
  - Employees need data to manage risk/ costs/ wellness
  - Payers have limited data to pay claim (HCFA 1500 form)
  - Payers reluctant to release employer’s population data
- Drugs/ Devices:
  - Want patients to “test”
  - Data drives FDA approval
  - Need access to diversity/uniformity of patient populations

Technology, Design, Management

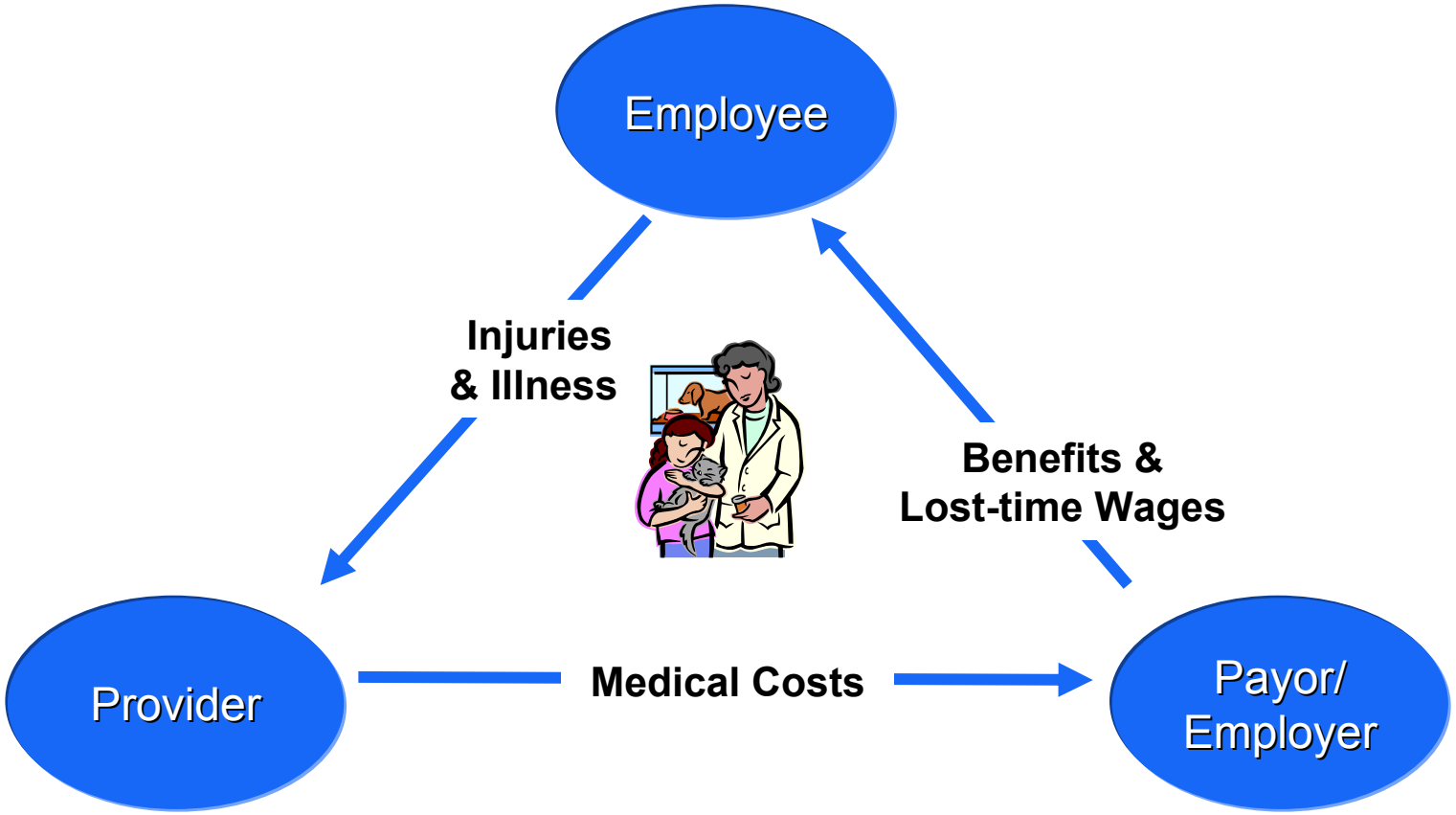
- Secure System Design:
  - System design is critical to security
  - Lack of pervasive security knowledge in healthcare
  - Need ability to maintain data on a federated basis
  - Patients “OWN” the data (as defined by HIPAA’s PHI definition)
  - Need ability to authorize access to “my health info” over heterogeneous systems and networks (a one2many, many2one problem)
- Grids, Operating Systems and Databases:
  - What is secure- a VOS (grid), an OS or a RDMS?
  - Does grid distribution facilitate security (e.g. security obscurity)?
  - The “master grid controller” as a point of failure?
  - Databases “lockdown” file structures to BIOS/ OS/ VOS, or not?
  - Local access vs. remote access?

The Real Problem

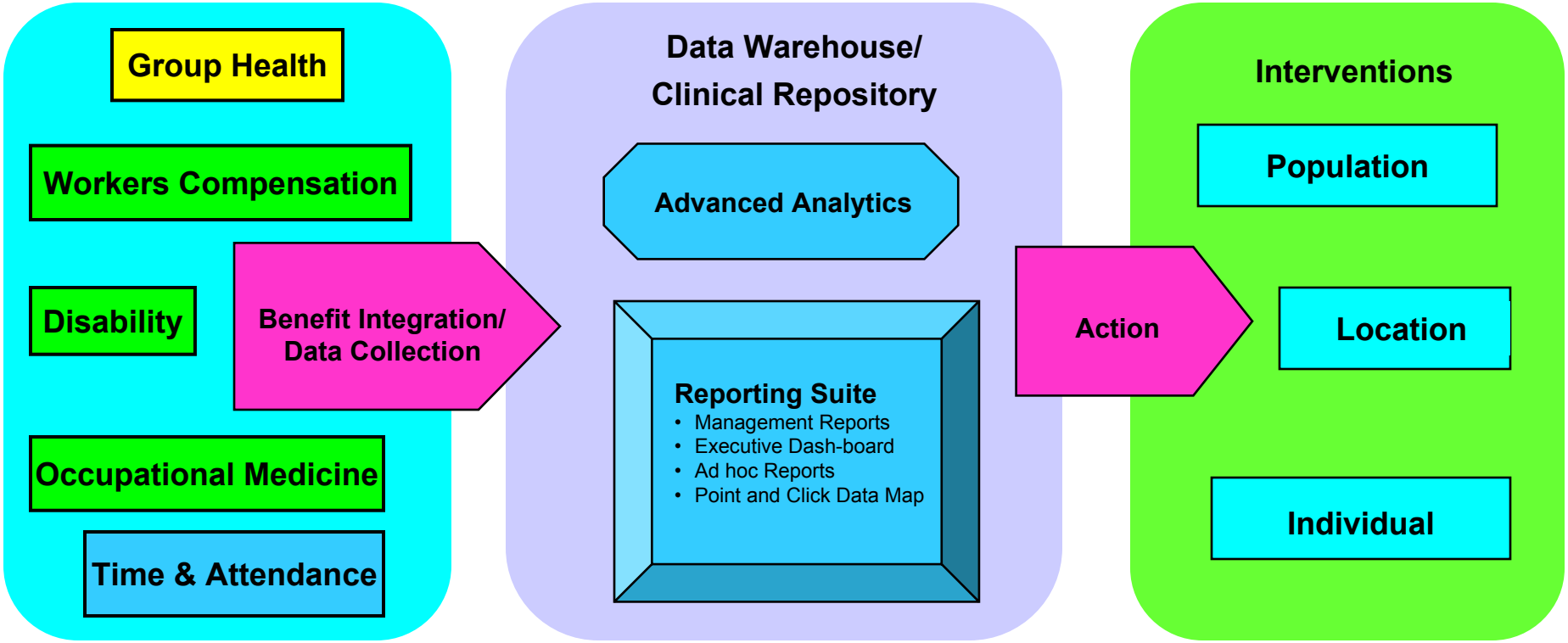
- Adoption:
  - How many of 785,000 providers have computer systems at work?
  - IF AMA's 98% physician Internet usage is accurate, how many even use computers in their office?
  - How many have or even know what an EMR is?
  - How many believe a "secure fax" locked in a closet is "good enough"?
- The Inside Job:
  - How many understand the importance of biometric systems?
  - How many use MS Windows 2003 with latest security updates?
  - How many providers meet DoD/ NSA security guidelines?
  - IF AMA's 98% physician Internet usage is accurate, how many even have a router or firewall?
  - Even if they have an EMR, how secure is it?
  - How many even have a policy on logins/ passwords or even know what to do with them?

Traditional Healthcare Environment

Group Health & Occupational Health Markets



Providing an Answer- Better Data Management



Clinical Data Collection and Integration

- Compile clinical data from all providers

Clinical Data Warehouse

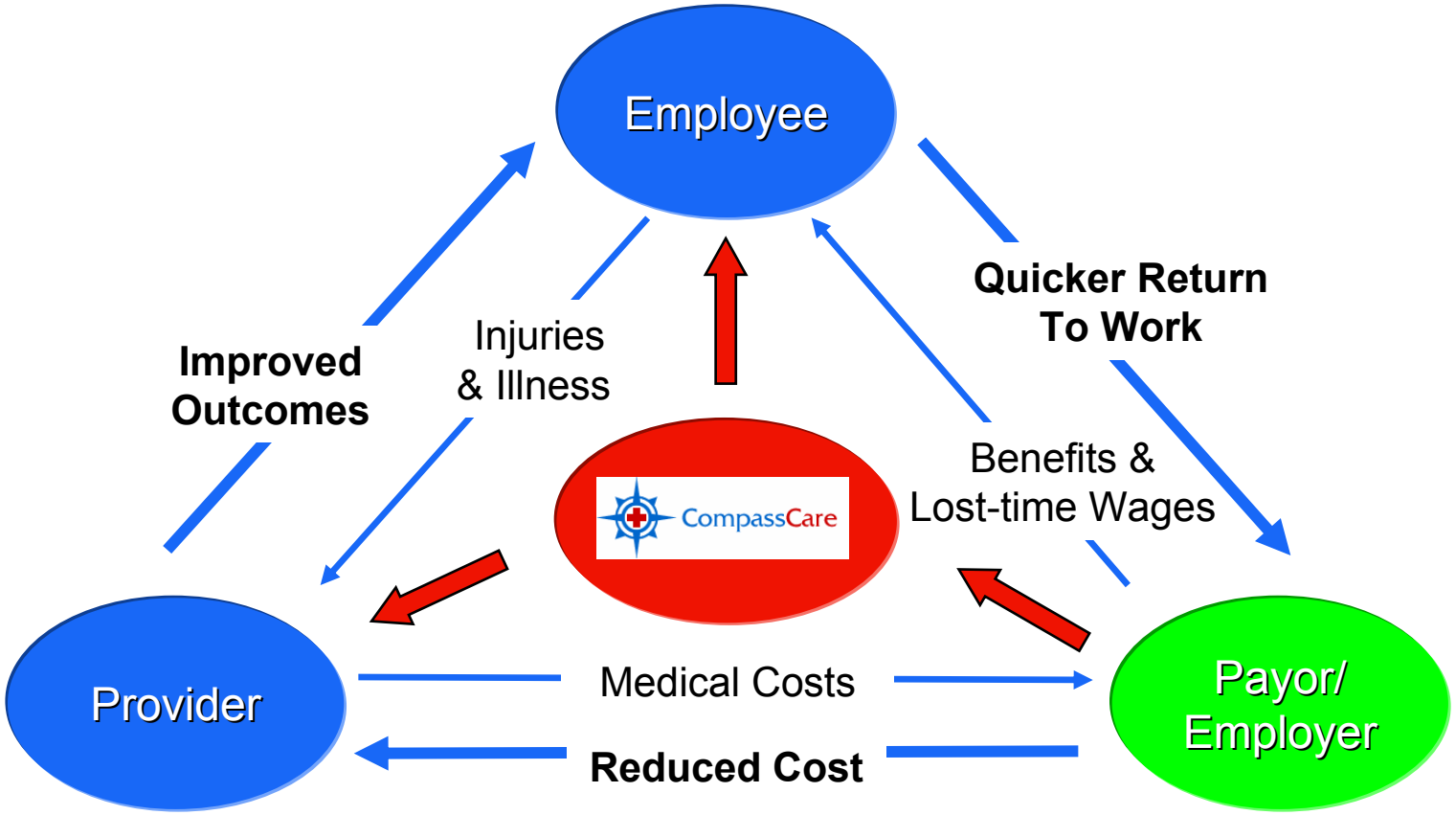
- Databases and systems designed for large-scale processing, transactional performance, high availability and “beyond HIPAA” security/ compliance

Interventions

- Real-time measurable data-driven interventions
- Prevention, mitigation, management, of disease

Connectivity Improve Outcomes & Costs

Workers' Compensation, Group Health & Occupational Health Markets

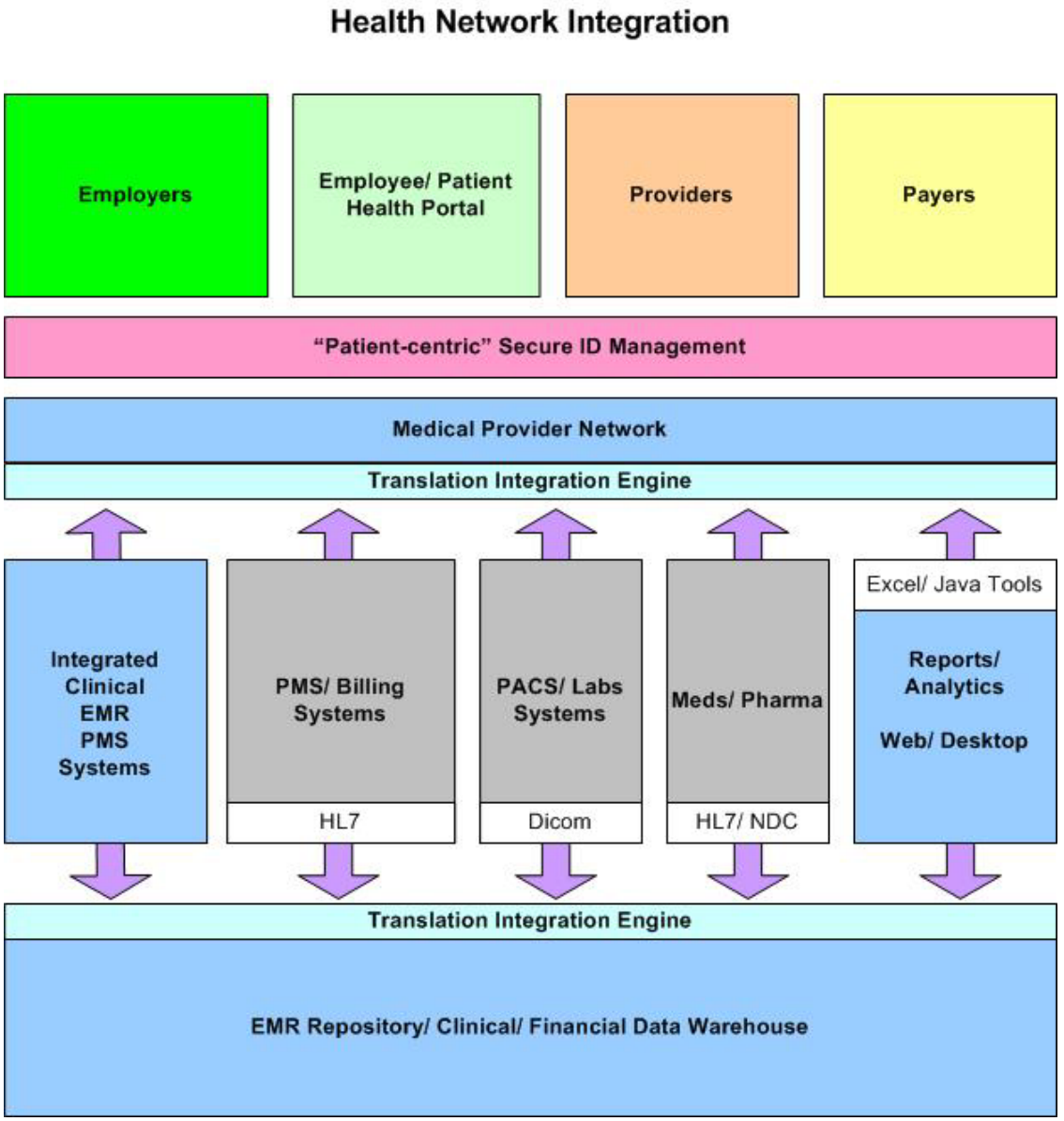


What's Required

An **integrated medical management information network** that empowers its customers to manage the quality and cost of healthcare through a unique blend of:

1. ***Powerful & Flexible Rules System -*** apply medical rules, business rules, financial rules and best practices medical guidelines to reduce medical and billing errors.
2. ***Workflow Automation Simplified -*** Reduces administrative burdens and bottlenecks. Enhances patient flow and expediency of treatment.
3. ***Real-time Employer Business & Clinical Rules -*** Employer protocols are handled discretely for appropriate medical intervention and process management.
4. ***Integrated Case Management Platform –*** Case managers, payers and employer/customers have real-time access to clinical data.
5. ***Enterprise-class Performance -*** Supports mission-critical health operations that require 99.9999% uptime, large-scale and "blink speed 300ms" response (a.k.a. the "grid").
6. ***HIPAA 2006 Security -*** Ensures customers of Dept. of Defense-level security down to the individual field in a medical record- "keystrokes" are tracked by all users.

What Must Be Delivered



Addressing the Solution with “Reasonable Efforts”

- Administrative:
  - What’s needed from personnel to administer health data
- Physical:
  - What’s needed for computers/ devices to help people manage health data
- Technical:
  - What’s really needed to make it all work

CompassCare

HIPAA-Grid requirements

Administrative Safeguards	Implementation Requirements
Security Management Process (164.308(a)(1))	Risk Analysis Risk Management Sanction Policy Information System Activity Review
Assigned Security Responsibility (164.308(a)(2))	Qualified Personnel Method to Determine Who It Is
Workforce Security (164.308(a)(3))	Authorization and/or Supervision Workforce Clearance Procedure Termination Procedures
Information Access Management (164.308(a)(4))	Isolating Health Care Clearinghouse Function Access Authorization Access Establishment and Modification

CompassCare

HIPAA-Grid requirements

Administrative Safeguards	Implementation Requirements
Security Awareness and Training (164.308(a)(5))	Security Reminders Protection from Malicious Software Log-in Monitoring Password Management
Security Incident Procedures (164.308(a)(6))	Response and Reporting
Contingency Plan (164.308(a)(7))	Data Backup Plan Disaster Recovery Plan Emergency Mode Operation Plan Testing and Revision Procedure Applications and Data Criticality Analysis

CompassCare

HIPAA-Grid requirements

Physical Safeguards	Implementation Requirements
Facility Access Controls (164.310(a)(1))	Contingency Operations Facility Security Plan Access Control and Validation Procedures Maintenance Records
Workstation Use (164.310(b))	Local/ Network access Remote/ Network access
Workstation Security (164.310(c))	Software (Application/ OS) Hardware (BIOS) Biometrics (ID)
Device and Media Controls (164.310(d)(1))	Disposal Media Re-use Accountability Data Backup

CompassCare

HIPAA-Grid requirements

Technical Safeguards	Implementation Requirements
Access Control (164.312(a)(1))	Unique User Identification Emergency Access Procedure Automatic Logoff Encryption and Decryption
Audit Controls (164.312(b))	Tracking Capability Reporting Capability
Integrity (164.312(c)(1))	Mechanism to Authenticate Electronic Protected Health Information
Person or Entity Authentication (164.312(d))	Role/ Responsibility Geographical/ Location-based Organizational Network
Transmission Security (164.312(e)(1))	Integrity Controls

Thank You!

Stuart Johnstone
CEO/ President
CompassCare Inc.
Lake Forest, IL
Ph. 312-224-2692
sjohnstone@compass-care.com