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
Defining the Problem

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.
Defining the Problem

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
Defining the Problem

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?
Defining the Problem

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

Employee

Provider

Medical Costs

Payor/Employer

Injuries & Illness

Benefits & Lost-time Wages
Providing an Answer - Better Data Management

Group Health

Workers Compensation

Disability

Occupational Medicine

Time & Attendance

Clinical Data Collection and Integration

• Compile clinical data from all providers

Data Warehouse/ Clinical Repository

Advanced Analytics

Reporting Suite

• Management Reports
• Executive Dash-board
• Ad hoc Reports
• Point and Click Data Map

Clinical Data Warehouse

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

Interventions

Population

Action

Location

Individual

Interventions

• Real-time measurable data-driven interventions
• Prevention, mitigation, management, of disease
Connectivity Improve Outcomes & Costs

Workers’ Compensation, Group Health & Occupational Health Markets

- Improved Outcomes
- Injuries & Illness
- Medical Costs
- Reduced Cost
- Benefits & Lost-time Wages
- Quicker Return To Work

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


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

Health Network Integration

Employers
Employee/Patient Health Portal
Providers
Payers

“Patient-centric” Secure ID Management

Medical Provider Network

Translation Integration Engine

Integrated Clinical EMR PMS Systems
PMS/Billing Systems
HL7

PACS/Labs Systems
Dicom

Meds/Pharma
HL7/NDC

Excel/Java Tools
Reports/Analytics
Web/Desktop

Translation Integration Engine

EMR Repository/Clinical/Financial Data Warehouse

Copyright & Confidential- CompassCare Inc. 2005
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
## Administrative Safeguards

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

**HIPAA-Grid requirements**
## HIPAA-Grid requirements

<table>
<thead>
<tr>
<th>Administrative Safeguards</th>
<th>Implementation Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Awareness and Training (164.308(a)(5))</td>
<td>Security Reminders&lt;br&gt;Protection from Malicious Software&lt;br&gt;Log-in Monitoring&lt;br&gt;Password Management</td>
</tr>
<tr>
<td>Security Incident Procedures (164.308(a)(6))</td>
<td>Response and Reporting</td>
</tr>
<tr>
<td>Contingency Plan (164.308(a)(7))</td>
<td>Data Backup Plan&lt;br&gt;Disaster Recovery Plan&lt;br&gt;Emergency Mode Operation Plan&lt;br&gt;Testing and Revision Procedure&lt;br&gt;Applications and Data Criticality Analysis</td>
</tr>
</tbody>
</table>
## HIPAA-Grid requirements

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

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

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