Auditing EMR System Usage

You Chen
Jan, 17, 2013
You.chen@vanderbilt.edu
Health data being accessed by hackers, lost with laptop computers, or simply read by curious employees.
Current HIPAA Security Rules are not enough.

$675,000 for Privacy Violation

Jail Time for Malicious Accesses

California Hospitals Fined $675,000 For Privacy Violations: Jun 11, 2010

Hospital Employee Gets Jail Time For HIPAA Violation: Apr 29, 2010 Hospital employee sentenced to federal prison for 3-week long medical records spree.

UCLA Employee Indicted For Celebrity Privacy Violations: May 8, 2008 Hospital employee sells celebrity medical info to tabloids.
HIPAA Security Rules

• Administrative Safeguards
  — Administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic protected health information (PHI)

• Physical Safeguards
  — Physical measures, policies and procedures to protect a covered entity's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion

• Technical Safeguards
  — The technology and the policy and procedures for its use that protect electronic protected health information [PHI] and control access to it
Current State

Monitor VIPs (the Clooney effect-finding more attractive man)

Monitor employee-employee access

Follow-up on external suspicion

Spot checks
Technical Safeguards

• Access Control
• Audit controls: Implement systems to record and audit access to protected health information within information systems
  – Track & audit employees access to patient records
  – Store logs for ≥ 6 years
Access Control?

• “We have *-Based Access Control.”

• “We have a mathematically rigorous access policy logic!”

• “We can specify {context, team, temporal} policies!”
  (Georgiadis et al, 2001; Park et al. 2001;)

• “We can control your access at a fine-grained level!”

• “Isn’t that enough?”


Why is the Problem So Hard?

- Hospital system is inherently dynamic

**Roles**
- Multiple responsibilities
- Fuzzy “"
- Changing “"

**Teams**
- Situation dependent
- Constrained by availability
  “Can you work today?”

**Reason**
- Who defines the policies?
- Often Vague
- Cluttered by “multi-use” systems
But If You Let Them, They Will Come

• In March 2006, researchers carried out an investigation on hospitals in the Central Norway Health Region
• Users were assigned to an initial set of privileges and could invoke actualization, temporarily escalating their rights as necessary
• Such an access control system is feasible when the number of actualizations is small

This case:
• 53,650 of 99,352 patients actualized
• 5,310 of 12,258 users invoked actualization
• Over 295,000 actualizations in one month

<table>
<thead>
<tr>
<th>Role</th>
<th>Users</th>
<th>Invoked Actualization in Past Month</th>
</tr>
</thead>
<tbody>
<tr>
<td>Nurse</td>
<td>5633</td>
<td>36%</td>
</tr>
<tr>
<td>Doctor</td>
<td>2927</td>
<td>52%</td>
</tr>
<tr>
<td>Health Secretary</td>
<td>1876</td>
<td>52%</td>
</tr>
<tr>
<td>Physiotherapist</td>
<td>382</td>
<td>56%</td>
</tr>
<tr>
<td>Psychologist</td>
<td>194</td>
<td>58%</td>
</tr>
</tbody>
</table>

Aim of Access Logs Auditing

- Raw & Factual
  - Access Log (AL)

- Understood & Desired
  - Expected Model (EM)
    - Patient Information Protection
    - High Efficiency of Resource Allocation
    - Improve Quality of Patient Treatment
<table>
<thead>
<tr>
<th>Encounter number</th>
<th>Department</th>
<th>Patient</th>
<th>position</th>
<th>Reason</th>
<th>Relationship</th>
<th>User</th>
<th>Date</th>
<th>Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>442.0000726</td>
<td>NMH Resident/Fellow-CPOE</td>
<td>Resident- Inpatient Primary Service</td>
<td>OBSTETRICS</td>
<td>12/14/2010 14:06</td>
<td>Prentice 13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>442.0000726</td>
<td>Advanced Practice Clinician - C Nurse Midwife</td>
<td>OBSTETRICS</td>
<td>12/14/2010 14:22</td>
<td>Prentice 13</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>442.0000726</td>
<td>Patient Care Staff Nurse</td>
<td>Covering Staff Nurse</td>
<td>OBSTETRICS</td>
<td>12/14/2010 14:33</td>
<td>Prentice 13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>442.0000726</td>
<td>Patient Care Staff Nurse</td>
<td>Primary Staff Nurse</td>
<td>OBSTETRICS</td>
<td>12/14/2010 14:38</td>
<td>Prentice 13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>442.0000726</td>
<td>Maternal &amp; Fetal Medicine</td>
<td>NMH Physician-CPOE</td>
<td>Patient Care</td>
<td>OBSTETRICS</td>
<td>12/14/2010 14:52</td>
<td>Labor and Delivery</td>
<td></td>
<td></td>
</tr>
<tr>
<td>442.0000726</td>
<td>NMH Resident/Fellow-CPOE</td>
<td>Resident- Inpatient Covering Service</td>
<td>OBSTETRICS</td>
<td>12/14/2010 15:03</td>
<td>Prentice 13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>442.0000726</td>
<td>NMH Resident/Fellow-CPOE</td>
<td>Resident- Inpatient Consulting Service</td>
<td>OBSTETRICS</td>
<td>12/14/2010 15:20</td>
<td>Prentice 13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>442.0000726</td>
<td>Anesthesiology</td>
<td>NMH Anesthesia-CPOE</td>
<td>Anesthesiologist</td>
<td>OBSTETRICS</td>
<td>12/14/2010 15:47</td>
<td>Prentice 13</td>
<td></td>
<td></td>
</tr>
<tr>
<td>442.0000726</td>
<td>Patient Care Staff Nurse</td>
<td>Covering Staff Nurse</td>
<td>OBSTETRICS</td>
<td>12/14/2010 16:29</td>
<td>Prentice 13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>442.0000726</td>
<td>NMH Resident/Fellow-CPOE</td>
<td>Resident- Inpatient Consulting Service</td>
<td>OBSTETRICS</td>
<td>12/14/2010 17:20</td>
<td>Prentice 13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>442.0000726</td>
<td>NMH Resident/Fellow-CPOE</td>
<td>Resident- Inpatient Primary Service</td>
<td>OBSTETRICS</td>
<td>12/14/2010 18:56</td>
<td>Prentice 13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>442.0000726</td>
<td>Med Student-CPOE</td>
<td>Med Student- Inpatient Primary Service</td>
<td>OBSTETRICS</td>
<td>12/14/2010 19:10</td>
<td>Prentice 13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>442.0000726</td>
<td>Patient Care Staff Nurse</td>
<td>Coordinator</td>
<td>OBSTETRICS</td>
<td>12/14/2010 19:20</td>
<td>Labor and Delivery</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>442.0000726</td>
<td>Patient Care Staff Nurse</td>
<td>Primary Staff Nurse</td>
<td>OBSTETRICS</td>
<td>12/14/2010 19:46</td>
<td>Prentice 13</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Examples of Patient Diagnose Codes

<table>
<thead>
<tr>
<th>Patient study ID</th>
<th>Enc. deiden</th>
<th>Diagnose codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>442.0000726</td>
<td>1</td>
<td>12165, 65921, 65951, 66401, 66481, V270</td>
</tr>
<tr>
<td>442.0001714</td>
<td>1</td>
<td>V053, V3000</td>
</tr>
<tr>
<td>442.0002396</td>
<td>1</td>
<td>4019, 4111, 41401, 4142, 4739, 49390</td>
</tr>
<tr>
<td>442.0002775</td>
<td>2</td>
<td>1122, 20300, 25000, 27651, 40390, 5845, 5859, 591, 5933, V1005, V1046</td>
</tr>
<tr>
<td>442.0002775</td>
<td>1</td>
<td>1534, 185, 1962, 1974, 20300, 25000, 2809, 40390, 56089, 5849, 5859, 59080, 591, 78791, 7907</td>
</tr>
<tr>
<td>442.0003301</td>
<td>1</td>
<td>75408, 76529, V053, V3100</td>
</tr>
<tr>
<td>442.0004873</td>
<td>1</td>
<td>V270, V8535, 27800, 64911, 64971, 65841, 66401</td>
</tr>
<tr>
<td>442.0005024</td>
<td>1</td>
<td>4019, 72252, V1582</td>
</tr>
<tr>
<td>442.0005968</td>
<td>1</td>
<td>5990, 2724, 311, 4019, 44022</td>
</tr>
<tr>
<td>442.0006352</td>
<td>1</td>
<td>65971, V270</td>
</tr>
<tr>
<td>442.0007008</td>
<td>1</td>
<td>25000, 6144, 99859, V1042</td>
</tr>
<tr>
<td>442.0007371</td>
<td>1</td>
<td>V707, 2859, 33394, 4019, 71690, 74190, V420</td>
</tr>
<tr>
<td>442.0007707</td>
<td>1</td>
<td>30000, 49121, 51889, 60000, 7850</td>
</tr>
<tr>
<td>442.0007707</td>
<td>2</td>
<td>78052, V1083, 30001, 496, 0549, 1120, 2768, 30000</td>
</tr>
<tr>
<td>442.0008016</td>
<td>1</td>
<td>V053, V3001</td>
</tr>
<tr>
<td>442.0008405</td>
<td>1</td>
<td>2449, 25080, 4019, 41400, 42731, 4280, 60000, V4581, V5861</td>
</tr>
<tr>
<td>442.0009617</td>
<td>1</td>
<td>V053, V3000</td>
</tr>
</tbody>
</table>
Various Ways of Access Logs Auditing

- Accesses of EHR
- Attributes of Users and Patients
- Social Network
- Time Series
- Workflows
- Analysis
- Usable Rules
- Treatment/Access Patterns
Logs

Anomalous Users Detection - CADS (Community based Anomaly Detection System) and MetaCADS

Predicting Diseases

Alerting of Anomalous Treatment or Accesses

Recommend Community of Departments

Interaction Network of Departments

Social Analysis

Accesses of Users on Patients

Interaction Network of Users

User view

User level
Anomalous Users Detection - CADS (Community based Anomaly Detection System) and MetaCADS

Access level
Anomalous Accesses Detection - SNAD (Specialized Network Anomaly Detection)

Department view

Relation Rules of Departments

Community of Departments

Patient view

Alerting of Anomalous Treatment or Accesses

Predicting Diseases

Department Interaction Network of Departments
Uncovering Anomalous Usage of Medical Records via Social Network Analysis
Two Typical Attacks

(1) Anomalous users detection – user level

(2) Anomalous accesses detection – access level

Intruders have little knowledge of the system and the anticipated behavior

Intruders have complete knowledge of the system and its policies
Two general objects of health information system

U(Users)
- U₁
- U₂
- U₃
- U₄
- U₅
- U₆

S(Subjects)
- S₁
- S₂
- S₃
- S₄
- S₅
- S₆
- S₇

Behavioral Modeling

Accesses
Where are We Going?

User Level Anomaly Detection
Community Anomaly Detection System (CADS) and Its Extension MetaCADS

(IEEE TDSC)

Access Level Anomaly Detection
Specialized Network Anomaly Detection (SNAD)

(Security Informatics)


Social Networks are a Novel Approach to Discovery of Electronic Medical Record Misuse
CADS on Vanderbilt Dataset

Deviation

# of Accesses
CADS on Northwestern Dataset

Deviation

# of Accesses
Example Environments

Electronic Health Records (EHR)

- Vanderbilt University Medical Center “StarPanel” Logs
- 3 months in 2010
- Arbitrary Day
  - \( \approx 4,208 \) users
  - \( \approx 1,006 \) patients
  - \( \approx 1,482 \) diagnoses
  - \( \approx 22,014 \) accesses of subjects
  - \( \approx 4,609 \) assignments of diagnoses
Where are We Going?

- User Level: CADS and MetaCADS
  - Framework of CADS and MetaCADS
  - An Example of CADS
  - Experimental Evaluation
  - Limitation

- Access Level: Specialized Network Anomaly Detection (SNAD) (SI)
CADS and MetaCADS

Pattern Extraction (PE)

(a) Access Network Construction
(b) User Community Inference
(c) Assignment
(d) Complex Category Inference

Access Logs

User Communities

(f) Deviation Assessment
(e) Nearest Neighbor Discovery

Anomaly Detection (AD)

Deviation Scores for Users
Where are We Going?

• User Level: CADS and MetaCADS
  – Framework of CADS and MetaCADS
  – An Example of CADS
  – Experimental Evaluation
  – Limitation

• Access Level: Specialized Network Anomaly Detection (SNAD)
  (SI)
Distance via Weighted Euclidean Distance

Nearest Neighbor Network

Bipartite Graph -> Access Network of Users

Communities via Singular Value Decomposition

Distance via Weighted Euclidean Distance

Nearest Neighbor Network

Deviation Scores Calculation

<table>
<thead>
<tr>
<th>User</th>
<th>2-NN</th>
<th>Deviation</th>
</tr>
</thead>
<tbody>
<tr>
<td>u₁</td>
<td>u₂</td>
<td>u₃</td>
</tr>
<tr>
<td>u₂</td>
<td>u₄</td>
<td>u₅</td>
</tr>
<tr>
<td>u₃</td>
<td>u₁</td>
<td>u₂</td>
</tr>
<tr>
<td>u₄</td>
<td>u₂</td>
<td>u₅</td>
</tr>
<tr>
<td>u₅</td>
<td>u₂</td>
<td>u₄</td>
</tr>
<tr>
<td>u₆</td>
<td>u₁</td>
<td>u₃</td>
</tr>
</tbody>
</table>
How Do We Set “k”-NN?

• Conductance- a measure of community quality (Kannan et al)

\[
\psi(\beta) = \frac{2}{4}, \psi(\alpha) = \frac{2}{8}, \psi(\gamma) = \frac{2}{\min\{4,12\}}
\]

\[
\psi(\alpha) < \psi(\beta) = \psi(\gamma)
\]
Minimum conductance at $k=6$
The average cluster coefficient for this network is 0.48, which is significantly larger than 0.001 for random networks.

Users exhibit collaborative behavior in the health information system.
Measuring Deviation from k-NN

- Every user is assigned a radius $r$:
  - the distance to his $k^{th}$ nearest neighbor
- Smaller the radius $\rightarrow$ higher density in user’s network

$$Dev(u_i) = \sqrt{\frac{\sum_{j \in k\text{nni}} (r_j - \bar{r})^2}{k}}$$

$$\bar{r} = \frac{\sum r_j}{u_j \in k\text{nni}}$$

$$\bar{r} = \frac{2 + 2 + 2 + 2 + 3}{5} = 2.2$$

$$Dev(q_1) = \sqrt{\frac{(2 - 2.2)^2 \times 4 + (3 - 2.2)^2}{5}} = 0.42$$

Radius for these points are nearly 2, and for $q_1$ is 3

Radius for these points are larger than 10, and every $r$ values significantly different

If we set threshold of radius as 10, than $q_1$ is a normal user, who in fact is anomalous
Where are We Going?

- User Level: CADS and MetaCADS
  - Framework of CADS and MetaCADS
  - An Example of CADS
  - **Experimental Evaluation**
  - Limitation

- Access Level: Specialized Network Anomaly Detection (SNAD)
  (SI)
Experimental Design

• Datasets are not annotated for illicit behavior

• We simulated users in several settings to test:
  – Sensitivity to number of records accessed of a specific users
    • Range from 1 to 120
  – Sensitivity to number of anomalous users
    • simulated users correspond to 0.5% to 5% of total users
    • Number of records accessed fixed to 5
  – Sensitivity to diversity
    • Random number of users(0.5%~5%) and records accessed (1~150)
Exp1: False Positive Rate Decreases, when the Number of Subjects Accessed Increases

MetaCADS achieves a smaller false positive rate than CADS. This is because the assignment network facilitates a stronger portrayal of real users’ communities than the access network in isolation.
Exp2: Detection Rate With Various Mix Rates of Real and Simulated Users

when the number of simulated users is low (i.e., 0.5 percent), MetaCADS yields a slightly higher AUC than CADS (0.92 versus 0.91)

As the number of simulated users increases, CADS clearly dominates MetaCADS. The performance rate of CADS increases from 0.91 to 0.94, while MetaCADS decreases from 0.92 to 0.87.

Because when the number of simulated users increases, they have more frequent categories in common. In turn, these categories enable simulated users to form more communities than those based on patients alone, thus lowering their deviation scores.
Exp3: MetaCADS dominates when the mix rate is low (mix rate = 0.5%)
MetaCADS deviation scores of real and simulated users as a function of the number of subjects accessed. This system was generated with a mix rate of 0.5 percent and a random number of subjects accessed per simulated user.
Where are We Going?

• User Level: CADS and MetaCADS
  – Framework of CADS and MetaCADS
  – An Example of CADS
  – Experimental Evaluation
    – Limitation

• Access Level: Specialized Network Anomaly Detection (SNAD) (SI)
Some Limitations

• Simulated users are indicative of misuse of the system... ...but actual illicit behavior may be more directed.

• “False positives” are not necessarily false! (Adjudication by EHR privacy experts under way)

• Need to specialize tool to account for semantics of users and subjects
  – User: {Role, Department, Residence}
  – Patient: {Diagnosis, Procedure, Demographics, Residence}

• Anomalous users... not anomalous accesses
  – Need to account for insiders that deviate by only a couple of actions
Where are We Going?

- User Level: CADS and MetaCADS
- Access Level: Specialized Network Anomaly Detection (SNAD)
  
  (SI)
  
  - Framework of SNAD
  - An Example of CADS
  - Experimental Evaluation
  - Limitation
SNAD Framework

- Similarity Measurement
- Access Network Measurement
- User Modeling
- Access Network Construction

- Anomaly Evaluation
  - Access Measurement
  - Anomaly Detection

- Access Logs

Anomaly Scores for Accesses
Where are We Going?

• User Level: CADS and MetaCADS

• Access Level: Specialized Network Anomaly Detection (SNAD)

(SI)
  – Framework of SNAD
  – **An Example of SNAD**
  – Experimental Evaluation
  – Limitation
User Modeling

\[ IDF(u_i) = \log \left( \frac{|S|}{1 + |\{s_j, \text{ where } SU(j, i) > 0\}|} \right) \]
Access Network Construction

- Similarity Measurement
- Access Network Measurement
- User Modeling
- Access Network Construction

Graph: Nodes represent users (U1, U2, U3, U4, U5, U6) and server (S1, S2, S3, S4, S5, S6, S7). Connections indicate relationships between users and servers.
Access Network Measurement

\[ Sim(u_i, u_j) = \frac{U_i \cdot U_j}{||U_i|| \times ||U_j||} \]
Measuring Accesses for Changes in Network Similarity

Access: $u_1 \rightarrow s_3$

<table>
<thead>
<tr>
<th>Network</th>
<th>Similarity</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>$u_1, u_2, u_4, u_5, u_6$</td>
<td>0.59</td>
<td>5</td>
</tr>
<tr>
<td>$u_2, u_4, u_5, u_6$</td>
<td>0.64</td>
<td>4</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Access</th>
<th>Score</th>
<th>Size</th>
</tr>
</thead>
<tbody>
<tr>
<td>$u_1-s_3$</td>
<td>0.05</td>
<td>4</td>
</tr>
</tbody>
</table>
Where are We Going?

• CADS and MetaCADS

• Access Level: Specialized Network Anomaly Detection (SNAD)
  (SI)
  – Framework of SNAD
  – An Example of SNAD
  – **Experimental Evaluation**
  – Limitation
Experimental Design

• Datasets are not annotated for illicit behavior

• We simulated users in several settings to test:
  – Sensitivity to number of subjects accessed
    • Range from 1 to 1,00
  – Sensitivity to number of anomalous users
    • Range from 2 to 20
    • Number of subjects accessed fixed to 5
  – Sensitivity to diversity
    • Random number of users and subjects accessed
SNAD: Detection Rate Increase with Number of Subjects Accessed
SNAD: Detection Rate Increases with Number of Intruders
SNAD Outperforms Competitors When the Number of Intruders & Accessed Subjects is Random
Where are We Going?

- CADS and MetaCADS

- Access Level: Specialized Network Anomaly Detection (SNAD)

  (SI)
  - Framework of SNAD
  - An Example of SNAD
  - Experimental Evaluation
  - Limitation
Limitations

• SNAD has high performance in Vanderbilt’s EHR system because
  – organization is collaborative
  – access networks have high network similarity

• SNAD may not be appropriate for large access network with low network similarity
  – Absence of a user has little influence on the similarity.

![Graph showing similarity of network vs size of network]
Conclusions

• It is an effective way by using social network analysis to detect anomalous usages of electronic health records, such as CADS and SNAD

• Adding semantic information of users and subjects will make social network analysis be more understandable
Protecting Patients through Dynamic Network Analysis of Hospital Department Relationships

Patient information needs to be protected from insiders

• Traditional security practices (e.g., role-based access control) are insufficient to ensure EMR security
  – Common for >100 employees to access a patient’s medical record during their visit
  – Often difficult to determine who the members of a care team are and who will need access to what information at which time
EHRs have adopted collaborative capabilities to facilitate interaction between teammates and coordinate care

• We hypothesize that HCO departments will exhibit predictable interaction behavior

• Our goals:
  1. Investigate if such behavior exists
  2. If so, determine if it is stable
     • If stable interactions become unstable \(\rightarrow\) associated patients will be anomalous
Our goal is to retrieve the dependent relations of departments and determine whether the dependencies among departments touching that patient are expected?

Expected behavior:
Pediatric housestaff; pediatric cardiology; Vanderbilt Children’s hospital

Utilized behavior:
Mental health center; burn center; breast cancer center; pediatric housestaff; pediatric cardiology; Vanderbilt Children’s hospital

The dependent relations between green departments and red departments are very low
Healthcare Interaction Networks

Tripartite graph of departments, users and patients

Bipartite graph of departments and patients

Health interaction network

Local view for p₆

Global view
Where are We Going?

**A Global Network of Departments**

Two metrics: certainty and reciprocity

Stable status in terms of the two metrics

**Local Network-for a specific patient**

Two metrics: local network score and reciprocity

**Application of the Networks**

Detecting patients with anomalous medical records accesses
Certainty to Model Relationship of Global Network

Cert(Lifeflight event medicine (d₃)->Emergency medicine (d₁)) = 4/4
Cert(Inpatient medicine(d₂)->Inpatient medicine(d₂)) = 6/7
Using reciprocity to characterize the mutual interaction between all pairs of departments in the global network

Reciprocity = 1

Pediatric Emergency Dept -> Peds Respiratory Care = 0.57

Peds Respiratory Care -> Pediatric Emergency Dept = 0.037
Where are We Going?

**A Global Network of Departments**

Two metrics: certainty and reciprocity

Stable status in terms of the two metrics

**Local Network-for a specific patient**

Two metrics: local network score and reciprocity

**Application of the Networks**

Detecting Patients with Anomalous Medical Records Accesses
Dataset used for this study

- Vanderbilt University Medical Center “StarPanel”
- 3 months in 2010
- Arbitrary Week
  - ≈ 9,200 users
  - ≈ 99,000 patient records
  - ≈ 400,000 accesses
  - ≈ 450 departments
Although the relations of the network are very unbalanced, the unbalance is stable over time.

<table>
<thead>
<tr>
<th>Time</th>
<th>Week 1</th>
<th>Week 2</th>
<th>Week 3</th>
<th>Week 4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reciprocity</td>
<td>0.267</td>
<td>0.2814</td>
<td>0.2858</td>
<td>0.2871</td>
</tr>
</tbody>
</table>

\[
\frac{(0.2814 - 0.267)}{0.267} = 0.05
\]

Week 1 to week 2
The changes become smaller over time (centralization: green > blue > red)

Degree of relations between departments changes little over time

>82.5% of the change resides in [-0.25, 0.25]
Strong relations between VUMC departments over a four week period

<table>
<thead>
<tr>
<th>Department (d_i)</th>
<th>Department (d_j)</th>
<th>Min Certainty</th>
<th>Max Certainty</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Intradepartmental Relations</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4East OB/GYN</td>
<td>4East OB/GYN</td>
<td>0.74319</td>
<td>0.7669</td>
</tr>
<tr>
<td>Adult Emergency Medicine</td>
<td>Adult Emergency Medicine</td>
<td>0.74024</td>
<td>0.78453</td>
</tr>
<tr>
<td>Cancer Infusion Center</td>
<td>Cancer Infusion Center</td>
<td>0.73171</td>
<td>0.844</td>
</tr>
<tr>
<td>8N Inpatient Medicine</td>
<td>8N Inpatient Medicine</td>
<td>0.7197</td>
<td>0.80909</td>
</tr>
<tr>
<td>Newborn Nursery</td>
<td>Newborn Nursery</td>
<td>0.70406</td>
<td>0.72727</td>
</tr>
<tr>
<td><strong>Interdepartmental Relations</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DOT Radiology</td>
<td>Orthopaedics</td>
<td>0.99621</td>
<td>1</td>
</tr>
<tr>
<td>Nursing Education and Development</td>
<td>Medical Information Services</td>
<td>0.95833</td>
<td>1</td>
</tr>
<tr>
<td>Main OR - Trauma/Renal</td>
<td>Medical Information Services</td>
<td>0.94444</td>
<td>1</td>
</tr>
<tr>
<td>Life Flight Event Medicine</td>
<td>Emergency Medicine</td>
<td>0.90805</td>
<td>1</td>
</tr>
<tr>
<td>Emergency Medicine Admin</td>
<td>Adult Emergency Medicine</td>
<td>0.91489</td>
<td>0.94186</td>
</tr>
</tbody>
</table>
Where are We Going?

**A Global Network of Departments**

Two metrics: certainty and reciprocity

Stable status in terms of the two metrics

**Local Network-for a specific patient**

Two metrics: local network score and reciprocity

**Application of the Networks**

Detecting patients with anomalous medical records accesses
Healthcare Interaction Networks

Tripartite graph of departments, users and patients

Bipartite graph of departments and patients

Health interaction network

Local view for $p_6$
Evolution of Local Networks in Terms of Local Network Score and Local Network Reciprocity

Each point in $P_{\text{start}}$ corresponds to a local network.
Over 98% of patients are normal because they exhibit a score change <0.05
Approximately 99% of patients are normal because they have a change of reciprocity <0.1
Where are We Going?

**A Global Network of Departments**
- Two metrics: certainty and reciprocity
- Stable status in terms of the two metrics

**Local Network-for a specific patient**
- Two metrics: local network score and reciprocity

**Application of the Networks**
- Detecting patients with anomalous medical records
- accesses
p2 has -0.93 change of local network score and -0.79 change of local reciprocity from the 1st to the 2nd week
Conclusions

• We hypothesized an HCO would exhibit strong stability → confirmed by our experiments

• We can characterize how strange a patient’s local network appears
  – Two groups of patients; those with small changes in local network score and reciprocity score and those with significant changes
  – The changes in the latter group do not justify the claim that the patient has been intruded upon, but may provide a reason for an investigation that incorporates more nuanced domain knowledge
Some Limitations

• Global and local networks appear to represent the business processes of HCO departments
  – however, such claims must be confirmed with employees knowledge about the working of the medical center and its affiliated clinics

• Need to specialize tool to account for semantics of patients
  – Patient: \{Diagnosis, Procedure, Demographics, Residence, physical location in a hospital\}

  – Incorporating semantics about the patient, $p_2$ in the last figure may have no intrusion; rather it is likely a complex cancer patient, which could be confirmed by inspection of clinical documents in the medical record
Thanks!
SNAD assumes that access scores are approximately distributed around a well-centered mean.
The correlation coefficient between real and Laplace distribution is 0.886.