Transforming a Privacy Program with Advanced Data Analytics
Session 74, February 21, 2017, 8:30 am to 9:30 am, OCCC 331A
Dr. Peter Greene, CMIO, Johns Hopkins
Robert Lord, Co-Founder and CEO, Protenus
Speaker Introduction

Peter Greene, MD

CMIO

Johns Hopkins Health System
Conflict of Interest

Peter Greene, MD

Has no real or apparent conflicts of interest to report.
Speaker Introduction

Robert Lord
Co-Founder and CEO
Protenus
Conflict of Interest

Robert Lord

Salary: Yes, Protenus
Royalty:
Receipt of Intellectual Property Rights/Patent Holder: Yes, Protenus
Consulting Fees (e.g., advisory boards):
Fees for Non-CME Services Received Directly from a Commercial Interest or their Agents (e.g., speakers’ bureau):
Contracted Research:
Ownership Interest (stocks, stock options or other ownership interest excluding diversified mutual funds): Yes, Protenus
Other:
Agenda

• Learning Objectives (2 min)
• STEPs (5 min)
• Johns Hopkins’ Decision to Move to Proactive Privacy Analytics (10 min)
• Detailing a New Analytical Paradigm (10 min)
• Tangible Lessons Learned and Results (5 min)
• Steps of Evolution of a Privacy Program (10 min)
• Summary of Benefits (3 min)
• Q&A (15 min)
Learning Objectives

• Compare traditional vs. innovative approaches for HIPAA violation identification and analysis
• Identify features that define appropriate and inappropriate user access to patient data
• Illustrate and provide examples of the five phases of advanced patient privacy monitoring
An Introduction of How Benefits Were Realized for the Value of Health IT

• **E=Electronic Information/Data**
  - Able to detect many new threats
  - Accuracy of detection completely unprecedented

• **S=Patient Satisfaction**
  - Increased community trust and reputation
  - Reduced friction between patients and institution as investigations were proactive and completed immediately

• **S=Savings**
  - Privacy programs are costly, labor-intensive
  - Breaches and mistakes result in average $2.2M cost/breach
    - huge fines
    - litigation
    - revenue loss
  - Patient satisfaction knowing their data are protected
    - Lower churn
Trust as a Strategic Priority

• Trust underlies everything that we sell in healthcare

• Proactive privacy analytics initiative decision made to “lift a fog” of mistrust and ambiguity around patient data
  – No visibility into how data was used, and if that use was appropriate

• Security and privacy are two key enablers of trust, which is the true goal
Importance of Trust

• Johns Hopkins holds trust as one of its most important strategic assets
  – Trust between providers and patients
  – Trust among workforce members
  – Trust between the community and the institution
• EHRs inherently present a challenge to trust
  – Deployed widely (access by employees, BAs, and affiliates)
  – Difficult to verify appropriate access (interconnected devices, BYOD, etc)
Raising the Bar on Patient Privacy

• The reality is that HIPAA is not enough
• Minimum requirements from OCR aren’t sufficient to ensure trust
• We were tired of just “checking the box”
Interactive Question #1

My org. is doing enough to ensure patient privacy and trust.

1 = Yes

2 = No
My org. is doing enough to ensure patient privacy and trust.

Start the presentation to activate live content
If you see this message in presentation mode, install the add-in or get help at PollEv.com/app
Original State of Program at Johns Hopkins

- Retroactive investigations
- Random audits
- Rule-based audits
  - Last-name match
  - Students
  - Nightly monitoring of local news
  - Other internal processes
- Lots of data to protect, highly manual processes
Who Was Responsible for Audits

• Privacy team
  – Waited for phone calls
  – Performed random audits of EHR access logs
  – Hard-working, highly-capable, but under-resourced and not technology-enabled

• IT supported privacy in ad hoc manner
  – Built simple rules-based queries
  – Assisted privacy however they could
Organizational Shift in Responsibility

• Due to a number of organizational catalysts and a perception of a changing landscape, privacy became a greater strategic priority
  – Office of the President
  – C-Suite of the Health System
  – Board of Directors
  – Our “Data Trust” Committee
• We wanted to reimagine what privacy could look like in an ideal world
Core Concerns of Leadership

• More employees in our health plan seeking care inside our delivery system
  • Angst of employees
• Board of Director members with specific privacy concerns around particular incidents
  • Broader rollout of systems to more community affiliates
Our Requirements for Change

- Change needed to be a paradigm shift, not an incremental change
- Needed to fundamentally change our “Trust Posture”
- Tangible metrics we wanted to improve
  - Proactively discover more threats (and types of threats)
  - Reduce false positives (huge waste of time)
  - Reduced # of tools that require maintenance, training, etc.
  - Reduce investigation times
  - Overall # of threats reduced over time
What Was Explored

- Automating rule-based system
  - Seemed to have significant false positive problem and we were doing this already
- Hiring additional staff
  - Planned, but costly
- Home-grown analytical systems
  - Some results, but hard to purpose-build with available tools and resources
  - Repurposing generic log file aggregation systems not appropriately tailored
Legacy Systems: Still Fishing Around

- Pre-specified data extracts
- Limited number of sources
- Hard-to-design rules-based analysis
- Pre-specification of the search
- High false positives
- Performance
- Visualization tools lacking
- Historical reporting often not present
Interactive Question #2

False positives are an issue in my organization.

1 = Agree        2 = Disagree
False positives are an issue in my organization.

Agree

Disagree

Start the presentation to activate live content
If you see this message in presentation mode, install the add-in or get help at PollEv.com/app
A New Option Emerged

• Different approach available from a team experienced sophisticated analytics
• Initial proof that we could algorithmically separate “appropriate” from “inappropriate” accesses with a low rate of false positives
• The opportunity for the complete paradigm shift that we mentioned, rather than an incremental change
• But was it just a “Shiny New Thing”?
Implementing Took Teamwork

- Initial rollout was a highly iterative process
- Side-by-side work with privacy, technology, and security team
- Close collaboration with data scientists and hands-on feedback into the system
- Purpose-built product for Privacy teams
**Vote of Confidence**

Early side-by-side results

<table>
<thead>
<tr>
<th>Family Member Privacy Violation Analytics Comparison</th>
<th>Last Name Match</th>
<th>Protenus Analytics</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number of Days Analyzed</td>
<td>6</td>
<td>6</td>
</tr>
<tr>
<td>Total Number of Alerts Produced</td>
<td>1127</td>
<td>69</td>
</tr>
<tr>
<td>Number of Cases Reviewed</td>
<td>364</td>
<td>69</td>
</tr>
<tr>
<td>Number Identified as Questionable</td>
<td>76</td>
<td>69</td>
</tr>
<tr>
<td>Number Identified as Not Questionable</td>
<td>288</td>
<td>0</td>
</tr>
<tr>
<td>Number of Questionable Identified as Violations</td>
<td>63</td>
<td>67</td>
</tr>
<tr>
<td>Number of Questionable Identified as Not Violations</td>
<td>13</td>
<td>2</td>
</tr>
</tbody>
</table>

| Percent Reviewed                                    | 32%             | 100%              |
| Percent Questionable                                | 21%             | 100%              |
| Percent Violation                                   | 17%             | 97%               |
| False Positive Rate                                 | 83%             | 3%                |
| Total Initial Case Review Time (hours)              | 80              | 6                 |
| Initial Case Review Time Per Violation (minutes)    | 76.2            | 5.1               |
Nothing’s Perfect – Challenges

• New workflows between IS and Privacy
• Number of threats increased significantly in short-term
• New capabilities raise new questions on “alert” meaning – what does it mean when alerts are this accurate?
• Need for buy-in from
  – data stewards
  – IT (who will support the platform)
• Requirement for significant computational power (cloud or in-network, both have own considerations)
Traditional Auditing Techniques Only Capture the “Tip of the Iceberg”
Privacy Analytics Platforms

- No data extract
- Any number of dimensions of analysis ("features" in Machine Learning)
- Any number of sources to enrich data (PACS, HR, pharmacy, etc.)
- Wide array of analytical techniques
- No need to specify what you’re looking for – can look for “anomalies”
- Few false positives
- Visualization speeds investigations 20-50x
- Reporting to demonstrate ROI
New Analytical Paradigm

• Alert accuracy currently so high that we trust the veracity of the alerts
• Understanding of workflows vastly aids investigation
• Multiple views data tell a story how users move through the HER
  − Privacy professionals ultimately judge between “appropriate” and “inappropriate” uses of the system
• With a “big data” platform, we examine and visualize an array of data that before had to be laboriously investigated
Useful Features and Sources

- Relationships between users (who collaborates frequently with whom?)
- Patterns of activity (how do individuals traverse the medical record)
- Patterns of treatment (what types of activities do people perform from a clinical perspective)
- What type of patient is being treated (so which types of providers should see them?)
- Typical anomaly detection tools (frequencies and times of day)
- The key is how to synthesize these like privacy professional
Questionable and Appropriate Accesses to Multiple Patient Records By One Employee Over 3 Months Time

Access Classification
- Appropriate
- Questionable

Patient Date of Birth
- Adult Patients
- Pediatric Patients

Number of Patient Records Accessed
Importance of Validation and Continuous Testing
Privacy Analytics as a Continuum

- Instructive to think about privacy analytics as a continuum, with four incremental steps, and one paradigm-shifting leap

Where are you?

nothing

Paradigm shift
Phase 1: Nothing

- Unfortunate truth is many institutions don’t have the time to really perform audits of their EHR audit logs in any substantive way

- Often times, hard-working teams don’t have the executive buy-in and staff to build out a monitoring program, despite what 45 CFR 164.308(a)(1)(ii)(D) and 45 CFR 164.312(a-d) mandate
Phase 2: Spot Audits

- Really just a “snapshot”
- Once per month, year, or quarter, taking a sample of users and auditing their work
- Maintain credibility and potentially put one just within the bounds of compliance
- Unlikely to yield much, given the huge number of accesses per year and the time it takes to investigate
Phase 3: Rule-Based Audits

- A wide array of potential tools
- Simplistic, but can get the job done
- Often require a lot of up-front rules specification
- Drowning in false-positives
Phase 4: Privacy Intelligence

- A wide array of tools purport “intelligence”
- Often adds a ROI component or dashboards
- Key is how the tools work together, move beyond more data, truly provide insight
Phase 5: Privacy Insight

- Clinical context
- Machine learning-driven evolution
- Ability to integrate data sources from throughout enterprise
- Use of ensemble anomaly detection
- Dynamic and interactive visualizations
- Supports privacy professionals
Interactive Question #3

Where are you on the continuum?

1  2  3  4

Nothing  Paradigm shift
Where are you on the continuum?

Start the presentation to activate live content
If you see this message in presentation mode, install the add-in or get help at PollEv.com/app
Whatever You Implement Should

- Track categories of breaches to understand sources
- Create standardized collaboration workflows
- Automate portions to overcome non-human scale problem
- Communicate platform to workforce
- Inform targeted education
Interactive Question #4

I think differently about patient privacy in my organization.

1 = Agree  2 = Disagree
I think differently about patient privacy in my organization

Agree

Disagree

Start the presentation to activate live content
If you see this message in presentation mode, install the add-in or get help at PollEv.com/app
Lessons We Learned

• Know where you are, decide your goals, and create a roadmap for the future

• This isn’t easy. Time, capital, and political capital all may be necessary.

• Thinking about Trust, rather than just Privacy, Security, or Compliance, is so much more powerful institutionally

• Get the institution energized – we generated palpable excitement throughout the institution by bringing in new groups, connecting groups that normally didn’t work together, and driving forward a mission that we all owned together
STEPS: Satisfaction

- Increased community trust and reputation
- Decrease in time to resolve patient privacy complaints
STEPS: Electronic Secure Data

- **1600% more inappropriate events detected**
- **False positive rate dropped from 85% to 3%**
STEPS: Savings

- More time to focus on non-investigation tasks (80 min -> 5 min per investigation)
- Decreased need to hire additional auditing staff
Questions

• Peter Greene, MD
  • pgreene@jhmi.edu

• Robert Lord
  • robert@protenus.com
  • @robertklord, @Protenus

Please complete your online session evaluation!