Guard Patient Privacy with Data Analytics

Brandon Neiswender
VP and COO, CRISP
December 5th, 2016
Transforming Healthcare through technology and collaboration

- VP, COO of Maryland HIE, CRISP
- 20+ years of Health IT and HIE leadership experience
- Formerly with St. Luke’s University Hospital Network and Erikson Community Retirement Communities
- MPH candidate, Loyola University Chicago
- MBA, Loyola University Maryland
- BS in Information Technology, University of Phoenix
What is CRISP?

- Maryland’s HIE, serves 60+ hospitals and healthcare organizations
- Serves over 8 million patients
- A national leader among HIEs, pioneering advancements in technology and analytics - delivers query portal, encounter notification, etc.
- 27,000 active users, thousands of independent physician organizations
- The future of information-sharing in healthcare
Threats to HIEs: A Basic Landscape

- There exist an ever-increasing number of threats to patient data
- Numerous organizations and providers in multiple locations
- Creates considerable challenges in making sure data is kept safe and assessed appropriately
Keeping Us Up at Night: High-Risk Scenarios

- VIP snooping
- Employees snooping on friends and family
- Stolen credentials
- General HIE system misuse/surfing
- Criminal Insiders
- Contractors
- Excessive use of query system
Healthcare Privacy Monitoring Issues

- CRISP uniquely situated as a hub - this isn’t just an HIE problem

- All healthcare organizations
  - Fear of “unknown unknowns” – not casting a wide enough net
  - False positives
  - Investigations still very inefficient and costly

- HIE-specific
  - Need to be delivering value, not just false alarms or noise
  - Huge amounts of transactions, often with less context or incomplete data
Existing Situation and Options

- Legacy system in place that we’ve outgrown and was not keeping up with our needs and the pace of our evolution
- We knew we needed something better, and explored evolving our current infrastructure and custom development
- While it takes more money up front, in the long-term you have a system that works and you’re saving on personnel and wasted time
Privacy Analytics System Requirements

● Large # of transactions = need for “big data” solutions

● Clinical context to provide leverage to investigations

● Need to build a unique profile of each user and patient and their respective behaviors

● High-level reporting and demonstration of efficacy with advanced visualizations

● Ability to easily and rapidly integrate new data sources and applications for analysis
Privacy Analytics Platform Implementation

- Implemented a new platform with clinical context and machine learning, detecting true threats to patient privacy.
- Now able to separate appropriate vs. inappropriate access to medical records with very few false positives.
- Can find types of threats that were not possible before and as well as determine when alerts are actually not a HIPAA violation.
Our Framework for Implementation

- Succinctly, we needed four elements to a new platform
  - Proactive
  - Personalized
  - Prioritized
  - Precise
Proactive

- Find threats that no one would have guessed could occur beforehand
- Identify threats before they cause problems
  - No need to specify rules or initiate investigations (though this can also be done)
- Before, CRISP relied on retrospective audits, driven by the limits and pre-specified rules of our previous system. This meant that complex threats weren’t detectable
Personalized

- Systems that learn over time, adapting to our institution and to the change/chaos of a clinical environment, becoming ever more accurate as it is used

- We weren’t capturing institutional knowledge of our own workflows and auditing processes before; now this is automated
Time and Activity of One Employee in 20 Medical Records

- Record A
- Record B
- Record C
- Record D
- Record E
- Record F
- Record G
- Record H
- Record I
- Record J
- Record K
- Record L
- Record M
- Record N
- Record O
- Record P
- Record Q
- Record R
- Record S
- Record T

Time in Record [Seconds]
Prioritized

- Not all threats are created equal, and we needed a system that could “triage” and provide individualized risk scores
- These risk scores could reflect separately the probability of a threat, as well as the level of risk
Precise

- Taking into account the unique circumstances of a user, in order to find threats that might otherwise not occur, and rule out incidents that are completely benign.

- Reduction of False Positives and False Negatives

- A flood of false positives with our previous system left us inundated – now we’re able to solely focus on the greatest threats to patient data in Maryland
Results

- Greater clarity into how PHI is being used across the region
- Detecting a greater number of threats with less overhead
- Can now efficiently and effectively resolve case investigations that used to take months in a matter of minutes
- Bottom line -> we’ve eliminated about 1500 hours of manual privacy work every year, while achieving exponentially greater benefits in our privacy posture
Additional Community Benefits

- Patients trust the system, share more with their providers, and ultimately receive better care
- Greater trust amongst our partner institutions
- Improved our reputation as a privacy and security leader
- Setting the tone for privacy requirements at the state and national level for HIEs
Key Takeaways and Recommendations

- Benefits of machine learning and big data analytics far outweigh those of rules-based systems
- Clinical context is key. Need to know the difference between a nurse and doctor, diabetic patient vs. ER admission, etc.
- Augmenting an existing team frees up time for other, more important initiatives – no longer drowning in audits
- Make the investment in more advanced analytics – TCO ends up being much lower, with much greater effectiveness
Q&A
Brandon Neiswender
CRISP
@branneis

boston.healthprivacyforum.com | #hitprivacy