C-Level Perspective: Reasonable Responses and Selling Your Plan

February 29, 2016
Conflict of Interest

David Levin, MD
Paul Connelly, MAMRD, CISSP

Has no real or apparent conflicts of interest to report.
Agenda

• CMIO and CISO perspectives: “Opposing” views??
• Collaboration: Working together for the greater good
  – Why the CISO can be the CMIO’s best friend
  – Why the CMIO can be the CISO’s best friend
  – Approaches
• Common Cases:
  – Medical device security
  – Data analytics
• Partnering to “sell” your plans to the Board
• Five take-away’s to try at your organization
• Q & A
Learning Objectives

• A CMIO’s view: Explain how to maximize the value of clinical IT at a time when medical systems and data are in the crosshairs of malicious outsiders and insiders

• A CISO’s view: Explain how to keep systems safe to protect your patients and organization, with many non-secure legacy systems, and threats, access, and dissemination of data growing exponentially

• Joint perspectives:
  – Discuss change drivers in healthcare (shift to value-based care, the rise of consumerism and changing patient expectations) and their effect on Security
  – Describe how changing healthcare needs mandate partnership between clinical and security leaders
  – Outline strategies for teaming up to “sell” secure solutions to the board and executive leadership
Benefits Realization With Health IT

Enabling the pursuit of the “Value Equation”

- Increased Quality
- Improved Safety
- Decreased Cost

For Patients, Providers and Payers!

http://www.himss.org/ValueSuite
CMIO View: From Volume to Value

• **Volume**: Today we get paid to do stuff. Do more stuff; get paid more regardless of results.

• **Value**: Tomorrow we will be paid based on the actual results, not for just doing stuff.

“If you can’t explain it to your mom and dad, you don’t really understand it.”
<table>
<thead>
<tr>
<th></th>
<th>Volume Based</th>
<th>Value Based</th>
</tr>
</thead>
<tbody>
<tr>
<td>Provider Incentive</td>
<td>Activity</td>
<td>Clinical Results &amp; Cost</td>
</tr>
<tr>
<td>Provider Payment</td>
<td>Fee for Service</td>
<td>Outcomes</td>
</tr>
<tr>
<td>Patient Role</td>
<td>Passive ; Dependent</td>
<td>Active; Engaged Partnership</td>
</tr>
<tr>
<td>Care Model</td>
<td>Acute; Episodic; Individual Patients.</td>
<td>Continuous; Chronic Disease; Prevention; Individuals and Populations</td>
</tr>
<tr>
<td>Provider Role</td>
<td>Silos of individual providers or groups</td>
<td>Collaboration; Medical Home; Teams; ACO’s</td>
</tr>
<tr>
<td>Analytics</td>
<td>Retrospective; Fragmented; Administrative</td>
<td>Real Time &amp; Predictive; Integrated; Clinical, Operational &amp; Administrative</td>
</tr>
<tr>
<td>Technology</td>
<td>Stand-alone EMR; Enables existing care models (cow paths)</td>
<td>True Interoperability; Enables new care models; Virtual care</td>
</tr>
</tbody>
</table>
Delivery of Clinical Services: The Three “P’s”

Personalized (Zoom In)
• Highly customized for each individual
• “Omics”, Real Time Info, Individual Needs & Tastes

Population-based (Zoom Out)
• Systems designed to care for large groups of similar patients

Pervasive (Zoom Everywhere)
• Ubiquitous; Everything connected
A CISO’s View: Daunting Risk

• Evolution of threats—
  – Today’s big data *thefts* may be remembered as the good old days; system and data destruction and attacks on people via cyber means for extortion and terrorism could become reality

• Impacts of decisions made in the past—
  – Living with an installed base with vulnerable systems-- a legacy of past clinical/business decisions

• The challenge— keeping pace with clinical/business pursuit of best and newest tools, innovations, uses of data—
  – Systems showing up on the loading dock, purchased with no security vetting, architecture, implementation plan, or maintenance/lifecycle provisions
  – Data analytics— who is getting what data; in mass quantities!

• Need to change the paradigm— Get security “baked in” to selection, purchasing, implementation, operation, and lifecycle
Our Objectives

• CISO—
  – I need to be involved from the start
  – I want to build in security and governance
  – I want to enable safe, effective, and efficient patient care

• CMIO—
  – I want to create more effective and efficient patient care
  – I want to find innovation opportunities
  – I want to protect my patients by ensuring security is part of it

• Wait a Minute!!
  – Did you say you want secure systems?!?
  – Did you say you want to improve patient care?!?
Why the CISO Should be a CMIO’s Best Friend

• “Secure” solutions carry more weight with management today—better chance of approval of initiatives when the CISO is onboard
• Working together from the start saves money, increases speed to market
• Collaboration on messaging to end-users creates right processes and drives adoption.
• Protects your patients—provides for privacy, integrity, and availability of the data/systems you need to provide care
• Protects you—
  – Two of three patients would not go back to a provider who breached their data
  – Regulatory compliance, litigation
  – Protection of Intellectual Property
Why the CMIO Should be a CISO’s best friend

• The CMIO can help you see around the corner—being involved in new initiatives and innovations from the beginning make security work better
• Your credibility across the organization—improves when you are integrated with the clinical team
• CMIO can help deliver security messages to end-users and leadership
• Help CISO improve their understanding of how the delivery of HC works and how security fits in
• Motivation for CISO team: you are part of a health care innovation
• Get away from being called “Dr. No” by demonstrating how you can be part of innovation and solutions
• Provide you a connection to work better together with other clinical and business leaders
Approaches to Collaboration

• Bringing the CMIO’s perspectives into security issues
  – Security governance council
  – Business decisions
  – Quarterly portfolio reviews
  – Checkpoint on IT purchase decisions, implementations

• Examples:
  • Setting standards for public Cloud services
  • Use of Smart devices
  • Use of personal devices
  • Authentication requirements
  • SSO deployment / Password requirements
  • SSN protection
Approaches to Collaboration (Cont.)

• Bringing the CISO into CMIO activities
  – Involve in clinical IT strategy, planning, implementation
  – Joint planning/presentations to key governance and stakeholder groups
  – Model collaborative behavior for others: make clear that you are partners

• Rounding in your facility—seeing how patient care is delivered

• Establish Pattern of Regular Interaction:
  – How will you get new ideas/plans in front of one another?
  – Keep the focus on the organizational goals
  – “Honor” one another’s perspectives for the greater good
Example: Jointly Driving Medical Device Security

• How the CMIO can support the CISO
  – Identifying the strategic priorities and critical systems—identifying where an attack could potentially be life-threatening to patients or damaging to the organization.
  – Changing legacy approach to purchasing, implementation, operation, and lifecycle planning
  – Gaining business support to mandate security from vendors

• How the CISO can support the CMIO
  – Vetting of vendors and products as part of the purchasing process
  – Identifying the security vulnerabilities and remediation plans to protect individual systems
  – Developing network architectures and access controls to protect medical devices
Example: Data Analytics

• **CMIO perspective:** Tremendous opportunity for improving effectiveness and efficiency of patient care; the more data the better; countless ways to use it

• **CISO perspective:** “Warning--Danger Will Robinson!” Mixing data from different sources, broad dissemination, ability to reconstruct personal information, putting all your jewels in one place makes it a bigger target

• **Approaching it together**—
  
  – Collaborate on the strategy—how can we reap the benefits within reasonable risk?
  
  – Identify the points of risk—where can we accept some risk in exchange for the patient care benefits? What are the stopping points?
  
  – Key controls—Collaborate to make system access, data governance, and other key control decisions *informed business decisions*
  
  – Jointly sponsor—discuss with leadership to show it requires both roles for success, present the risks and rewards
Partner to Sell Secure Health Care Innovations

• Audience: Leadership, Providers and Patients!
• The days of HC organizations “blindly” buying new technologies, i.e., without the CMIO’s and the CISO’s blessing need to be in the past
• Looking forward— CMIOs and CISOs need to be key partners
  – Balance, judgement
  – Risk vs opportunity
  – Art & Science
  – Collaboration to meet each other’s goals
  – Every dollar spent on security is a dollar not devoted to patient care
Engaging the Leadership and the Board

**Big Picture:** Always show a view that balances risk with strategic objectives.

**Stewardship:** Bring complete solutions that are cost effective and align with organizational goals

**Impact:** Show benefits of investments & the cost “doing nothing”

- Use of standards like the NIST CSF, magic quadrant—highest bang for the buck
- Help establish security position for Clinical initiatives
Leadership and the Board: CSIO/CMIO Collaboration

Nothing kills credibility faster than being “A Silo Expert”
- CISO who only sees security objectives
- CMIO who only sees clinical or business objectives

Be able to show CMIO-CISO collaboration and support for security initiatives
- At every stage from concept to design to delivery/maintenance
- Deliver on promises
  - Jointly make projects a success
  - Avoid surprises when both have been engaged from the start

**Bonus Advice:** Same approach works for CFOs, Legal Counsel, and others who job is to “hug a pole”
Five Take-Aways: Do Try This at Home

1. Define your CISO/CMIO Collaboration process—How you make it happen at your organization:
   – Collaboration via committees, regular 1:1 check-ins, joint sign-offs on new initiatives

2. Communications—Send messages to the organization that you are aligned:
   – Sending CISO messages via CMIO channels
   – Sending CMIO messages about clinical care and innovation in security messages
Five Take-Aways: Do Try This at Home (cont.)

3. Walk a mile in one-another’s shoes
   - Carve out time to shadow one-another via rounding, join the other’s staff meeting, etc.
   - Build a better understanding and appreciation for the other’s goals, challenges, priorities

4. Engage Leadership Together
   - Give a joint CMIO/CISO state of the union message to your leadership
   - Pick a project and “work the messaging to leadership” together.

5. Tackle the Human Factors – Work together to understand and remediate human factors (behavior) that contribute to a more secure environment.
Value Depends on Security

• For Patients, Providers and Payers!

• Essential for the pursuit of the “Value Equation”
  – Increased Quality
  – Improved Safety
  – Decreased Cost

http://www.himss.org/ValueSuite
Discussion

Paul Connelly
VP of Information Protection
Chief Information Security Officer
Hospital Corporation of America

Dave Levin, MD
Chief Medical Officer
Sansoro Health
Dave@SansoroHealth.com
@SansoroHealth