


June 15-16, 2010
GOVERNMENT
HEALTH IT conference & exhibition
HIMSS

Innovation 2010:
On the Threshold of Meaningful Use

The Need for a National Healthcare Security Framework

Erik Pupo
Health Interoperability Architect

VANGENT 
Inspired Thinking. Powerful Results.

www.govhealthitconference.com

June 15-16, 2010
GOVERNMENT
HEALTH IT conference & exhibition
HIMSS

Innovation 2010:
On the Threshold of Meaningful Use

- Goals for today:
 - What is the specific problem we are trying to solve with a national healthcare security framework?
 - What are the specific risks and issues we see from not having a healthcare security framework in place nationwide?
 - Is FISMA the answer to the problem?
 - What could we do FISMA to make it work as a healthcare security framework?
 - What are the immediate next steps needed?

www.govhealthitconference.com

June 15-16, 2010
GOVERNMENT
HEALTH IT conference & exhibition
HIMSS

Innovation 2010:
On the Threshold of Meaningful Use

The depth of damage caused by a lack of security controls can wreck the trust fabric essential to the adoption of health IT

www.govhealthitconference.com

June 15-16, 2010
GOVERNMENT
HEALTH IT conference & exhibition
HIMSS

Innovation 2010:
On the Threshold of Meaningful Use


- Its not just trust, its reputation:
 - Once trust is compromised, an organization's reputation is damaged. One of the biggest risks for any HIE or other health IT provider/vendor is reputational risk
- HIE's, Hospitals, Providers, and Specialists risk being "Lehmanized" – remember them?
 - We won't share information with you
 - We won't let you store information about patients we give you
 - We look at you as a higher "risk"

www.govhealthitconference.com

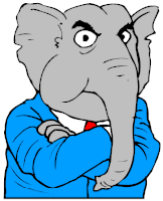
June 15-16, 2010
GOVERNMENT HEALTH IT conference & exhibition
powered by HIMSS

Innovation 2010:
 On the Threshold of Meaningful Use

- But aren't there a ton of security frameworks already that can solve this issue?



YES and NO!



So why do we need a new way to look at this problem?

www.govhealthitconference.com

June 15-16, 2010
GOVERNMENT HEALTH IT conference & exhibition
powered by HIMSS

Innovation 2010:
 On the Threshold of Meaningful Use

- There is a big gap in aligning current security frameworks to healthcare and to “meaningful use” of health IT
 - We have no minimal set of guidelines from the federal government in support of meaningful use “risk analysis”
 - We have the perception from outside the government that FISMA is an OMB-mandated paperwork exercise that lacks real-time threat monitoring
 - We have no current educational program to help practices and hospitals understand what CMS is looking for to meet security meaningful use requirements

www.govhealthitconference.com

June 15-16, 2010
 GOVERNMENT HEALTH IT CONFERENCE
 conference & exhibition
 HIMSS

Innovation 2010:
 On the Threshold of Meaningful Use

- In theory, there are multiple solutions to this challenge:
 - Myriad number of security frameworks to choose from so the healthcare industry can choose whatever they want
 - Large numbers of consultants and services available to support these frameworks
 - Create government programs to educate the healthcare industry on FISMA
 - Update the IFR on meaningful use to more fully set out minimal guidelines for risk analysis

www.govhealthitconference.com

June 15-16, 2010
 GOVERNMENT HEALTH IT CONFERENCE
 conference & exhibition
 HIMSS

Innovation 2010:
 On the Threshold of Meaningful Use

- But what is really feasible?
 - No one framework can currently meet the needs of all the different stakeholders in the healthcare industry
 - The disparities in frameworks can weaken the overall “trust fabric” needed to support information exchange
 - There is “healthcare fatigue” on Capitol Hill – no one wants to “mandate” anything
 - There is no funding available to educate stakeholders on FISMA – you are “on your own” 😊
 - OMB may never come out with guidance understandable to everyone

www.govhealthitconference.com

June 15-16, 2010
GOVERNMENT
HEALTH IT CONFERENCE
conference & exhibition
powered by HIMSS

Innovation 2010:
On the Threshold of Meaningful Use

- So why not FISMA as the healthcare security framework?
 - Currently, federal medical agencies that handle patient data must comply with FISMA. If they want to share that data, the recipients also may need to comply with FISMA
 - CMS, for example, applies FISMA to approximately 200 contractors, including 15 Medicare contractors that process and pay the 1.2 billion Medicare claims annually

www.govhealthitconference.com

June 15-16, 2010
GOVERNMENT
HEALTH IT CONFERENCE
conference & exhibition
powered by HIMSS

Innovation 2010:
On the Threshold of Meaningful Use

- The problems with FISMA as the solution
 - There is a difference between control monitoring and threat monitoring
 - FISMA is currently viewed as security control compliance monitoring
 - Mandating inputs versus assessing outputs
 - FISMA is perceived as control-focused, which does not translate well to a physician or hospital environment
 - FISMA is designed for a certain set of scenarios and is designed by the government
 - It was never designed from the perspective of a specific industry and its security needs

www.govhealthitconference.com

June 15-16, 2010
 GOVERNMENT
HEALTH IT CONFERENCE
 conference & exhibition
 HIMSS

Innovation 2010:
 On the Threshold of Meaningful Use

- The problems with C&A
 - The C&A process is not optimized for external healthcare use:
 - Basically, preparing a Certification Package is **writing about security**. When you are preparing a Certification Package, you usually **don't perform any sort of hands-on security**. You review the existing security design and architecture documents, interview various IT support and development folks familiar with the infrastructure, and document your findings.
 - It IS optimized for consultants ☺ - but healthcare organizations don't have infinite budgets

www.govhealthitconference.com

June 15-16, 2010
 GOVERNMENT
HEALTH IT CONFERENCE
 conference & exhibition
 HIMSS

Innovation 2010:
 On the Threshold of Meaningful Use

- The “Are You Nuts!!!!!!” Problem?
 - FISMA has 171 controls, HIPAA has 101 of those FISMA controls – which one do I follow?
 - Data that moves from a federal computer system to a private sector system is still considered federal data under current OMB guidance (August 2008)
 - Legal views vary on whether NHIN participants must comply with FISMA
 - Imagine applying that legal interpretation to the entire nation

www.govhealthitconference.com

June 15-16, 2010
GOVERNMENT HEALTH IT CONFERENCE
 conference & exhibition
 HIMSS

Innovation 2010:
 On the Threshold of Meaningful Use

- What we are risking with FISMA
 - The threat of “Security Theater”
 - The appearance of security to make patients and providers feel better about information exchange without actually securing their data.
 - The threat of the checkbox
 - I check off a box saying I have implemented a control without actually continuously monitoring that control.
 - The threat of C&A paperwork
 - Average packages can go to 500 pages and can take 1-3 years to complete

www.govhealthitconference.com

June 15-16, 2010
GOVERNMENT HEALTH IT CONFERENCE
 conference & exhibition
 HIMSS

Innovation 2010:
 On the Threshold of Meaningful Use

- So what do we do?
 - Nothing – allow providers to simply implement whatever framework they would like, as per a liberal interpretation of meaningful use requirements
 - Modify FISMA – since FISMA is the main security framework used by the federal government, modify it in a way that makes it more amenable for healthcare industry use
 - Create a “new framework” that harmonizes controls, procedures, and best practices from current frameworks and sets a minimum set of guidelines and controls

www.govhealthitconference.com

June 15-16, 2010
 GOVERNMENT HEALTH IT CONFERENCE
 conference & exhibition
 HIMSS

Innovation 2010:
 On the Threshold of Meaningful Use

- How FISMA could be the answer
 - The best approach would blend a framework like FISMA into actual hands-on penetration testing and evaluation
 - It would “modularize” FISMA to make it relevant to Federal-Private Sector exchanges without impeding Private Sector exchanges
 - It would require “provable” threat monitoring rather than basic risk assessment
 - It would set a minimal, base set of guidelines that can be drawn from NIST 800-53

www.govhealthitconference.com

June 15-16, 2010
 GOVERNMENT HEALTH IT CONFERENCE
 conference & exhibition
 HIMSS

Innovation 2010:
 On the Threshold of Meaningful Use

- How would this new “FISMA” for healthcare
 - Selecting controls for the healthcare industry that are effective and that make sense, and that assure trust between federal and private sector participants in information exchange.
 - Monitoring, detecting, and reacting to those controls would be the focus, not checklists and writing
 - Testing the effectiveness of the controls with periodic (and perhaps random) field assessments / “survival, penetration, integrity tests” would become the role of the government

www.govhealthitconference.com

June 15-16, 2010
GOVERNMENT
HEALTHIT CONFERENCE
conference & exhibition
powered by HIMSS

Innovation 2010:
On the Threshold of Meaningful Use

- What NIST 800-53 guidelines might be relevant to this new FISMA?
 - **Inventory of Authorized and Unauthorized Hardware.**
 - **Inventory of Authorized and Unauthorized Software.**
 - **Secure Configurations for Hardware and Software on Laptops, Workstations, and Servers.**
 - **Secure Configurations of Network Devices Such as Firewalls and Routers.**
 - **Boundary Defense**
 - **Maintenance and Analysis of Complete Security Audit Logs**
 - **Application Software Security**
 - **Controlled Use of Administrative Privileges**
 - **Controlled Access Based On Need to Know**
 - **Continuous Vulnerability Testing and Remediation**
 - **Dormant Account Monitoring and Control**

www.govhealthitconference.com

June 15-16, 2010
GOVERNMENT
HEALTHIT CONFERENCE
conference & exhibition
powered by HIMSS

Innovation 2010:
On the Threshold of Meaningful Use

- What other controls would be relevant?
 - **Anti-Malware Defenses**
 - **Limitation and Control of Ports, Protocols and Services**
 - **Wireless Device Control**
 - **Data Leakage Protection**
 - **Secure Network Engineering**
 - **Red Team Exercises**
 - **Incident Response Capability**
 - **Data Recovery Capability**
 - **Security Skills Assessment and Training to Fill Gaps**

www.govhealthitconference.com

June 15-16, 2010
GOVERNMENT
HEALTH IT CONFERENCE
conference & exhibition
powered by HIMSS

Innovation 2010:
On the Threshold of Meaningful Use

- **If the feds lead, the industry will follow:**
 - For pure business purposes, the industry will want to maintain a good information security posture
 - They don't want to be the "Bear Stearns" or "AIG" of health information exchange
 - But they want the feds to maintain a strong posture as well:
 - Only 3 of 24 agencies "pass" FISMA
- **By requiring everything, we will achieve nothing**

www.govhealthitconference.com