Lessons Learned – A Retrospective Discussion on HITRUST Certification

George Macrelli, HMS; Travis Good, Catalyze; Brad Carvellas, HM Health Solutions; Andrew Hicks, Coalfire; Cliff Baker, Meditology
Agenda

• Introductions

• HMS & HITRUST – Lessons Learned from a BA/CE’s Perspective

• HM Health Solutions & HITRUST – Lessons Learned from a BA/CE’s Perspective

• Catalyze & HITRUST – Lessons Learned from a BA’s Perspective

• Coalfire and Meditology – Lessons Learned from an Assessor’s Perspective

• Q&A
George M. Macrelli, HMS, Senior Director, Security Assurance

25 years of experience in the field of information technology and has a diverse background in both Technology Infrastructure and corporate Governance, with extensive experience in research, instructional, and enterprise computing, as well as Business Resilience.

At HMS, he oversees the Enterprise Security Assurance initiatives, which develops security governance programs, business resilience & continuity, and provides corporate security services. George has 15 years of information assurance practice experience, working in the financial services industry, healthcare, local government, and sports venues.

Since 1974, HMS has been enterprising healthcare, and provides a broad range of healthcare cost containment solutions in the industry – all to help payers improve performance.

Who We Serve

- Medicaid Managed Care Organizations
- Medicare Advantage plans
- Group and individual plans
- Self-funded employers
- Medicaid agencies
- CHIPs (Children’s Health Insurance Programs)
- State employee health benefit plans
- Centers for Medicare and Medicaid Services
- U.S. Department of Veterans Affairs
- Department of Defense

Our Competitive Advantages

- 100 million people under contract
- Unique access to vast datasets for analytics
- National footprint across hundreds of health plans, state agencies, and the federal government
- Broad range of solutions from pre-pay through recovery
- Solutions for health plans, state and federal agencies, and employers
- Delivery models from consulting through full outsourcing
Brad Carvellas, Director, Information Security and Risk Management
CISSP, CISM, ALMI

Brad is a technology, information security and risk management executive with 17 years of experience delivering risk-based information security solutions to national diversified health enterprises and Fortune 100 life and annuity insurance carriers.

Brad’s team lead HM Health Solutions and United Concordia Dental to HITRUST certification for their Health and Dental claims processing platforms in 2015.
• HM Health Solutions
  – Is a subsidiary of Highmark Health established in 2014 employing over 3000 employees
  – Provides a robust, cloud-based, multi-tenant platform that supports health insurance operations
  – The solution supports Commercial, Individual, Medicare and Medicaid lines of business

• Highmark Health
  – Is America's third largest integrated health care delivery and financing system
  – Employs more than 35,000 people and serves over 40 million Americans in all 50 states
Catalyze

TRAVIS GOOD, M.D.
Catalyze – Travis Good, M.D.

Travis Good, M.D., MBA, MS, CEO and Co-founder of Catalyze, Inc., is a speaker, blogger and expert in healthcare technology, specifically HIPAA compliance and security issues involved with healthcare innovation.

In addition to his work as CEO of Catalyze, which offers a compliant cloud-based infrastructure for enterprises and digital health developers, Dr. Good is also editor for industry blog HISTalkConnect, where he extensively reports on the innovations in healthcare technology.
About Catalyze

• Catalyze provides compliant, HITRUST-Certified tools to accelerate digital health adoption and scaling

• Catalyze products solve the two common challenges for digital health technologies:
  1. Data security and compliance; and
  2. Data exchange

• Catalyze supports a wide range of customers from providers (VA, MedStar), to payers (Blue Shield of California, Optum/United), to life sciences (Amgen), to digital health vendors (Healthloop, Propeller Health)
Andrew Hicks, Principal, Healthcare & Life Sciences
MBA, CISA, CCM, CRISC, HCISPP, HITRUST CSF Practitioner

Mr. Hicks has over 15 years of experience in IT governance including IT security, risk management, audit, business continuity, disaster recovery, and regulatory compliance.

His experience and understanding of business processes and technology provides expertise in the areas of policy development, internal control design and testing, project management, system development reviews, and risk mitigation.
Cyber Risk Strategy
Risk Advisory > Risk Assessment > Planning & Governance
Infrastructure & Staffing > Vendor management

Compliance & Regulatory Mandates
> Maintain compliance mandates
> Determine best fit for corporate objectives

Technical Testing & Analysis
> Test & adjust current defense controls
> Insights into identity, motives, and potential methods of attack

Threat Intelligence
> Exchange of emerging threats
> Advisory on risk acceptance and avoidance
> Delivery of intelligence information
Meditology

CLIFF BAKER
BACKGROUND & EXPERIENCE

- Exclusive to Healthcare
- Leadership with over 20+ years of industry experience
- Leaders that come from prominent Chief Security and Privacy Officer roles in industry
- Worked with 100's of business associates
- 60+ resources serving clients across the country
- 100+ HITRUST related clients in the past 5 years
- Trusted by nation’s largest health plans and providers to assist them with certification efforts

KNOWLEDGE & HITRUST FOCUS

- Accredited HITRUST CSF Assessor organization
- Meditology CEO was Chief Strategy Officer and Lead Architect for HITRUST CSF
- Proven methodology with supporting tools and templates
- Active as a HITRUST Alliance Partner working to update the CSF and facilitating industry leadership meetings
- Sought after HITRUST speakers at national industry and security conferences

www.meditologyservices.com
HMS and HITRUST

GEORGE MACRELLI
CE/BA Business Challenges

Compliance challenges in the healthcare vertical space includes:

- Dealing with recurring audits from multiple clients at the Federal, state, and commercial levels
- Customized questionnaires and varying control standards
- Governance and oversight for downstream vendors that perform outsourced business processes to HMS.

From a cultural perspective:
- Implementing adequate risk management oversight at all levels, balancing
- Product speed-to-market, ensuring that compliance goals and objectives are met.
Rationale/business drivers for HITRUST

1. HIPAA/HITECH
2. CLIENT and BUSINESS PARTNER REQUIREMENTS

- Notable clients have increasingly required the HITRUST CSF certification as a prerequisite for continuing to do business.
- By streamlining Risk Management and Governance under one common framework, allows for a consistent assessments approach, control monitoring, and transparent reporting to our stakeholders.
- From a sales and marketing perspective, CSF certification gives the organization a competitive advantage in the marketplace, allows us to respond to RFPs that contain strong security requirements faster.
High-level view of lessons learned

Being CSF certified is hard work, but with a high ROI!

- In-scope controls require periodic review to ensure they’re still operating effectively.
- It takes Executive commitment, and requires developing the technology, people, and processes to sustain compliance.
- Clients that are CSF certified sometimes have third-party audit staffers who aren’t as knowledgeable about HITRUST requiring additional work in education, and promoting the value of a certification.
- Changing the corporate culture to support CSF certification requires long-term engagement with stakeholders at all levels of the organization.
HM Health Solutions and HITRUST

BRAD CARVELLAS
Why HITRUST?

- Build, manage, measure and evidence an information security program benchmarked against an industry recognized risk-based controls framework
- Relying Parties and Third Parties realize value

HITRUST CSF is the most widely-adopted security framework in the U.S. healthcare industry
HM Health Solutions HITRUST Journey

• Assessment Scope
  – Claims Processing Systems
• Highmark Health Plan
• United Concordia Dental
HM Health Solutions Lessons Learned

• Roles, Responsibilities and Accountability
  – Management
  – Control owners

• Communication/Education
  – Value
  – Impact

• Project Management
  – Team
  – Timeline
  – Demand and Capacity
  – Metrics
Catalyze and HITRUST

TRAVIS GOOD, M.D.
Why did we choose HITRUST?

1. **Internal rigor.**
   - We wanted to force a level of information security and organizational structure into everything we do.

2. **External validation.**
   - We wanted to confidently say more than “we’re HIPAA-compliant”, we wanted to signal that we take information security management seriously and raise the standard in the industry.

3. **Marketing.**
   - We wanted to leverage HITRUST, and our experience using it, to generate content for, and add value to, our content marketing strategy.
HITRUST Lessons Learned

• Make an internal resource a HITRUST SME
  – You will reap the benefits pre-, peri-, and post-assessment

• Estimate effort, cost and timeline, then double it
  – There are 3 parties (you, assessor, and HITRUST) and you don’t want to be the bottleneck

• Focus on process, documentation, and management of your info sec program
  – HITRUST CSF requires more rigor in terms of process and implementation maturity

• It’s more than worth it. The ROI is only clear post-certification
Lessons Learned from an assessor’s perspective...

• It’s a journey, not a destination.
• You need a trusted partner, not an auditor.
• Domain expertise is essential.
• Client cross-training is imperative.
• Executive buy-in is key.
• It’s an investment in security, not a check-in-the-box compliance project.
Meditology and HITRUST

CLIFF BAKER
Meditology Lessons Learned

- Establish clear accountability within your organization
- Certification process will impact resource workload
- Defining the scope of the assessment can be a challenge
- Find an assessor that will partner with you each step of the way
- Focus on implementing a robust security function and avoid checklist sign-off strategies
- Don’t forget measured and managed processes
- Misconceptions about required capital investments
QUESTIONS
Contact Information

George Macrelli, HMS
gmacrelli@hms.com

Travis Good, Catalyze
travis@catalyze.io

Brad Carvellas, HM Health Solutions
brad.carvellas@highmark.com

Cliff Baker, Meditology
cliff.baker@meditologyservices.com

Andrew Hicks, Coalfire
andrew.hicks@Coalfire.com