Obtaining CSF Certification – Lessons Learned and Why Do It

Aaron Miri, Chief Technology Officer, Children’s medical Center of Dallas
Ryan Sawyer, Director, Technology Risk and Identity Governance, WellPoint
Kurt Hagerman, Chief Information Security Officer, FireHost
Andy Woods, Director, Regulatory Compliance and Risk, Availity
Obtaining HITRUST Certification

Why obtain certification and lessons learned

April 2014

Aaron Miri, Chief Technology Officer
Overview

• Why HITRUST certification

• Certification Process

• How did we get started?

• Lessons Learned
Overview

Mission: To make life better for children

Vision: Children’s will be among the very best medical centers in the nation

Background:
• Serves fourth largest metro area in U.S.
• Highest projected growth of pediatric population over next 20 years
• Three campuses: Dallas, Plano and Southlake with 559 licensed beds
• $1B in assets, $2B in gross revenue, AA3 bond rating
• Over 5,000 employees and 1,000 physicians
• Over 100K inpatient days, 300K outpatient visits, 100K emergency visits
• Academic affiliation with University of Texas Southwestern Medical School
• Only Level I pediatric trauma center in North Texas (1 of 22 in U.S.)
• Only U.S. pediatric hospital with six Joint Commission disease-specific certifications
• Nursing Magnet status; <10% of hospitals in nation have achieved
• Top 10 children’s hospital in nation (U.S. News & World Report 2009)

IT Recognition:
• 2013 HIMSS Enterprise Davies Award of Excellence Winner
• HIMSS EMR Adoption Stage 7; first hospital in Texas to achieve this level
• Top 200 U.S. companies by InformationWeek 500 for IT
• HITRUST Common Security Framework Certification
• Most Wired by Hospitals & Health Networks eight times
Why HITRUST CSF Certification?

The healthcare legislative landscape is constantly evolving

Legislative Milestones:

• 2013: Health Insurance Portability and Accountability Act (HIPAA) / Health Information Technology for Economic & Clinical Health (HITECH) Omnibus Final Rule
• 2013: Breach Notification Rule
• 2013: Texas House Bill 300 (TXHB300)
• 2010: U.S. Department of Health and Human Services (HHS) Guidance on Risk Analysis Requirements under the HIPAA Security Rule
• 2009: American Recovery and Reinvestment Act (ARRA) / Health Information Technology for Economic & Clinical Health (HITECH)
• 1996: Health Insurance Portability and Accountability Act (HIPAA)
Why HITRUST Certification

- Fines for non-compliance can be several million dollars
- Clear framework: Common Security Framework (CSF)
- Integrate information security risk management into overarching enterprise risk management programs

Demonstrate controls for HIPAA Compliance
Certification Process: CSF

Self-Assessment against CSF

HITRUST reviews for recommendation

Common Security Framework

Results submitted to HITRUST

Update and implement needed changes

3rd party assessment

HITRUST reviews for recommendation

Demonstration of Security Across an Organization
How did we get started?

- **Leadership**: It takes leadership from the top down in order to set the tone and the culture

- **Concept**: Must have buy-in at all levels of the organization, including the grassroots

- **Funding**: Organization must be willing to invest time and resources into people, processes, technology
Children’s-specific milestones for CSF

• Availability and dedication of Children’s resources to support

• Availability of relevant technical and non-technical staff for interviews and data gathering

• Onsite reviews of a sample set of MyChildren’s Clinics, Carrollton Data Center, Dallas main hospital, and Boulder disaster recovery facility

• Ability to rapidly respond to inquiries from HITRUST regarding assessment and validation

• Organizational patience and significant investment
Lessons Learned

- **Documentation**: Key for every process
- **Time**: The process can be lengthy and resource intensive
- **Savings**: Once the processes are engrained – your team is more efficient
- **Culture**: If you don’t refine your organizational culture, CSF certification becomes extremely difficult
- **Partnerships**: Internal & external partnerships critical
Why HITRUST for WellPoint

Highly regulated industry resulting in multiple compliance programs

Customers require extensive security questionnaires and audits

Control requirements and interpretations may vary depending on standard and company

CSF security framework aligns with healthcare industry requirements

• Consistent, structured, prescriptive and assures clients of our strong security practices
WellPoint HITRUST Certification Journey

Pre-Certification Assessment (late 2010/early 2011)

• Assessed against all CSF controls (135 at that time)
• A number of opportunities for enhancement identified.
• Prioritized remediation activities executed over a 24 month period

2013 Certification Assessment

• Assessed against 2013 CSF requirements utilizing new MyCSF tool and assessment methodology
• Organization factors required 282 baseline control statements across 19 domains
  – New scoring and assessment model required 1,410 written ratings and responses
Lessons Learned

Organizational Support

• Organizational buy-in from the top-down is key given cross functional needs
  – Critical to sustain focus on importance of the CSF

Communication

• Open channel between entity, assessor, and HITRUST is key to ensure consistent interpretation of requirements and expectations

Documentation

• Substantial documentation requirements on entity
  – Focus early to support a more efficient certification cycle

Formal Program

• HITRUST support program is necessary for long-term success and repeat certifications
Recognized Value of HITRUST Certification

Reputation

• Demonstrates focus on being a leader in the marketplace and trustworthy business partner
  – Instill greater customer confidence that their information is protected

Compliance

• Provide method for on-going compliance monitoring
  – Ensures alignment and adherence to security related regulatory requirements

Time and Cost Savings

• Reduces client and customer audit requests and internal assessment time.
• Average cost avoidance of ~300K each time certification can be used in lieu of performing an external assessment requested by client or customer
  – Recognized ~900K in cost avoidance in 2013
HITRUST Certification
The FireHost Journey

Kurt Hagerman
Chief Information Security Officer

HITRUST 2014
22 April, 2014
Kurt Hagerman

FireHost

Chief Information Security Officer

Kurt Hagerman oversees all compliance related and security initiatives. He is responsible for leading FireHost in attaining ISO, PCI, HIPAA and other certifications, which allows FireHost customers to more easily achieve their own compliance requirements. He regularly speaks and writes on information security topics in the payments and health care spaces as well as on cloud security.

Kurt Hagerman

Email  kurt.hagerman@firehost.com

Phone  +1 877 262 3473 x8073
Who is FireHost?

Security
FireHost's Intelligent Security Model™ provides multiple layers of protection from the physical data center all the way through to the database. Security is the core of FireHost's infrastructure, not something that's been bolted on.

Compliance
The FireHost infrastructure exceeds the compliance mandates for HIPAA and PCI DSS with a secure, validated cloud. This auditor friendly environment protects healthcare and payment businesses of all sizes from the risk of crippling cybercrime.

Performance
Only hardware, software, systems and configurations designed specifically for high performance, production workloads meet the entry criteria for FireHost's secure cloud. Secure servers are ranked #1 for performance in 3rd party benchmarks.

Service
Proactive support meets control and visibility. With over 24 distinct points of service, a robust API and a powerful portal, FireHost serves as an extension of any IT department. We take pride in providing automation with a human touch.
FireHost’s Security Validation

- Auditor and security assessment friendly infrastructure

**PCI DSS Compliant**
FireHost has been validated as a Level 1 Service Provider under PCI DSS for our services. Our validation includes specific PCI DSS controls on which customers can rely.

**HIPAA/HITRUST**
FireHost has been certified against the Common Security Framework (CSF) from the Health Information Trust Alliance (HITRUST) to address HIPAA security rule compliance requirements.

**SSAE 16 SOC 1 / SOC 2**
FireHost has received SOC 1 Type 2, SOC 2 Type 2, SOC 3 and ISAE 3402 reports. These reports demonstrate the viability of FireHost’s control program over time.

**ISO 27001**
FireHost has received a certificate of approval for our control program against the ISO/IEC 27001:2005 standard for Information Security Management Systems.
Why FireHost Got HITRUST Certified

• Security and Compliance are core values

• **Third party attestation** against a recognized controls framework focused on HIPAA security rule

• Added credibility to our security program

• Mapping of our controls to show how we help our customers achieve their own compliance with HIPAA

• Marketing and Sales
  • Too many CSPs tout being HIPAA compliant with no proof
  • Allows us to avoid the “trust us we’re compliant” messaging – we have a recognized certification
  • Differentiation from competitors that has helped us win business
OBTAINING CSF CERTIFICATION –

LESSONS LEARNED AND WHY DO IT?

Andy Woods
Director, Regulatory Compliance and Risk
Availity, LLC
BACKGROUND

• Founded in 2001, Availity is one of the largest health care information networks in the nation.

• The Availity Health Information Network® extends to more than 350,000 active providers; 2,700 hospitals; 575 vendor partners; and, all health plans nationwide.
CSF AT AVAILITY

• Obtained HITRUST Certification in 2011

• Just completed our second assessment cycle

• CSF internally used by:
  – Information Security
  – Privacy
  – Compliance
  – Risk Management
  – Internal Audit
WHY DO IT?

• CSF is a robust platform that consolidates:
  – Federal and state regulations
  – Industry standards and best practices
  – Trends in risk management

• Improves your ability to stay current:
  – Regular updates by HITRUST to reflect changes to regulations, standards, and trends
  – Provides a consolidated way to manage the multitude of changes

• Improves efficiencies:
  – Criteria and baseline requirements guide in the interpretation of regulatory requirements and application to business processes
  – Ensure all regulatory requirements and standards are considered in managing covered risks
  – Saves time and resources in tracking regulatory changes
  – Framework can be leveraged in responding to third-party audit requests
  – Enables efficient onboarding of new employees

• Demonstrates to Availity’s business partners the importance of privacy and security at Availity while supporting the flow of health care information
LESSONS LEARNED

• Where the **value** of the CSF is realized:
  – Policy, process, and implementation is the foundation for a compliant business
  – Measuring and managing to baselines is how you ensure compliance
  – Efforts must be focused on measuring and bringing visibility to the effectiveness of processes

• HITRUST certification gives additional rationale for the business in upholding high standards
  – Regulatory requirements are minimum expectations…we are holding ourselves to higher standards