



HITRUST CSF Assurance Program

Simplifying the Meaningful Use Privacy and Security Risk Assessment

Table of Contents

- Regulatory Background
- CSF Assurance Program – Simplifying the Risk Assessment
- CSF Assurance Program Overview
- Case Study

Presenters

- John Christiansen
 - Faculty, Information School at University of Washington
 - Managing Director/Attorney, Christiansen IT Law
- Michael Frederick
 - Chief Information Security Officer, Baylor Health Care System
- Cliff Baker
 - Chief Strategy Officer, HITRUST

Regulatory Background

Legal Background

- Roots of Meaningful Use
 - U.S. Office of National Coordinator for Health Information Technology (ONC) (est. 2004)
 - National Health Information Network (NHIN), regional and local health information organizations (RHIOs and LHIOs), interoperable electronic health records, EHR certification, etc.
 - Health Information Technology for Economic and Clinical Health Act (HITECH Act), part of American Recovery and Reinvestment Act of 2009 (ARRA)
 - Enhanced privacy and security protections, standards development and certification infrastructure for EHRs and health information exchange
 - Financial incentives for EHRs

Legal Background

- Financial incentives
 - Eligible professionals (EPs) may seek incentive under Medicare or Medicaid (not both)
 - Medicare: Up to \$18,000 in calendar year 2011 or 2012, to five year cap of \$44,000
 - Medicaid: Maximum of \$63,750 over six years, \$21,250 maximum in first year
 - Single employer (physician practice, etc.) may aggregate all EP incentives

Legal Background

- Financial incentives
 - Hospitals
 - Both Medicare and Medicaid possible
 - Complicated formula, base of \$2 million for up to 1,149 acute care inpatient discharges for prior 12 months, plus \$200 for each additional discharge up to 23,000, to maximum of \$6,370,200, plus transition factors
 - Multi-campus hospital systems under same provider number considered one hospital (with some adjustments)
 - Possible legislative fix in Congress

Legal Background

- Financial incentives
 - Must demonstrate compliance with meaningful use criteria
 - Stage 1 criteria: published in July 2010 (our current concern)
 - Stage 2 to be issued 2011
 - Stage 3 to be issued 2013

Legal Background

- How to get the money
 - Medicare hospitals' EPs must attest, through "secure mechanism approved by CMS," that they have "satisfied the required objectives and associated measures" of §495.6
 - Calendar years 2011 and after (no provision for demonstration), except that EPs using certified EHR need not attest until 2012
 - 42 CFR §§ 495.8; 495.210

Legal Background

- How to get the money

- Medicaid providers must attest:

“This is to certify that the foregoing information is true, accurate, and complete. I understand that Medicaid EHR incentive payments submitted under this provider number will be from Federal funds, and that any falsification, or concealment of a material fact may be prosecuted under Federal and State laws.”

(42 CFR §§ 495.368)

Legal Background

- 42 CFR §495.6 (a) (EPs) , (b) (hospitals): Stage 1 objectives and associated measures
- (d)(15)(EPs), (f)(14)(hospitals):
 - (i) **Objective.** Protect electronic health information created or maintained by the certified EHR technology through the implementation of **appropriate technical capabilities.**
 - (ii) **Measure.** Conduct or review a **security risk analysis** in accordance with the requirements **under 45 CFR 164.308(a)(1)** and implement **security updates** as necessary and **correct identified security deficiencies** as part of its **risk management process.**

Legal Background

- The “objective” is “appropriate technical capabilities”
- The “measure” is whether a HIPAA risk analysis has been conducted , “security updates” have been implemented and “security deficiencies” have been corrected
- Is the “risk analysis” only required to consider “technical capabilities?”
- **Probably not.**

Legal Background

- Measure: Can you attest that you have implemented/ complied with the Risk Analysis standard without looking at “non-technical” risks?
- The standard:
 - “Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.”
(45 CFR 164.308(a)(1))

Legal Background

- Measure: Can you attest that you have implemented “security updates” and “corrected security deficiencies” without looking at “non-technical” risks?
- The standard:
 - “A security update would be required if any security deficiencies were identified during the risk analysis. A security update could be updated software for certified EHR technology to be implemented as soon as available, to changes in workflow processes, or storage methods or any other necessary corrective action that needs to take place in order to eliminate the security deficiency or deficiencies identified in the risk analysis.”

Legal Background

- What are “appropriate technical capabilities?”
 - “The ONC final rule specifies certain capabilities that must be in certified EHR technology. For the objective we simply mean that a technical capability would be appropriate if it protected the electronic health information created or maintained by the certified EHR technology. All of these capabilities could be part of the certified EHR technology or outside systems and programs that support the privacy and security of certified EHR technology. We could not develop an exhaustive list.”
- “It depends.”

Legal Background

- HIPAA risk analysis standard
 - “The required risk analysis is also a tool to allow flexibility for entities in meeting the requirements of this final rule. The risk analysis requirement is designed to allow entities to look at their own operations and determine the security risks involved. The degree of response is determined by the risks identified.”
- **Application of HIPAA Risk Analysis to EHR technical capabilities for determination of appropriate updates and corrections requires analysis of EHR administrative, physical safeguards to identify possible technical risks**

Legal Background

- Risks associated with attestation
 - “A commenter indicated that attestation is an insufficient means to hold providers accountable for the expenditure of public funds and to protect against fraud and abuse.”
 - “We likewise are concerned with the potential fraud and abuse. However, Congress for the HITECH Act specifically authorized submission of information as to meaningful use through attestation. CMS is developing an audit strategy to ameliorate and address the risk of fraud and abuse.”

Legal Background

- Risks associated with attestation
 - CMS (Medicare) and states may “review an EP, eligible hospital or CAH’s demonstration of meaningful use.”
(42 CFR § 495.8)
 - States required to “annually collect and verify information regarding the efforts to adopt, implement, or upgrade certified EHR technology and the meaningful use of said technology before making any payments to providers.”
(42 CFR § 495.366)

Legal Background

- Risks associated with attestation
 - States required to
 - Ensure the qualifications of the providers who request Medicaid EHR incentive payments
 - Detect improper payments
 - Refer suspected cases of fraud and abuse to the Medicaid Fraud Control Unit
 - Take corrective action in the case of improper EHR payment incentives to Medicaid providers.
(42 CFR § 495.368)

Legal Background

- Risks associated with attestation
 - HITECH incentives audits
 - HIPAA compliance investigations
 - Security breach investigations
 - Federal/state false claims act penalties
 - Whistleblower (qui tam) lawsuits
 - Federal/state program disqualification
 - Criminal/civil fraud actions

Legal Background

- Managing risks associated with attestation
 - Risk analysis is a **process**, not a **product**
 - Follow HIPAA “flexible factors” and “reasonable and appropriate” standards in determining updates and corrections
 - Show due diligence in risk identification and update and correction implementation
 - Use appropriate professional expertise
 - Incorporate “best practices” information from industry, professional communities
 - Strongly consider use of outside expertise

Legal Background

- Supporting attestation
 - Make sure attesting officer is properly informed about risks, updates, corrections, etc.
 - Create and retain supporting documentation file
 - In any field where officer does not have appropriate expertise, ensure s/he is briefed and provided with supporting documentation from appropriate experts
 - Good “business judgment” is the attesting officer’s best friend
 - **Show your work!**
 - Document risk analysis process and findings
 - Document implementation of updates and corrections
 - Providers must retain “documentation supporting their demonstration of meaningful use for 6 years” after attestation
 - HIPAA has same document retention period

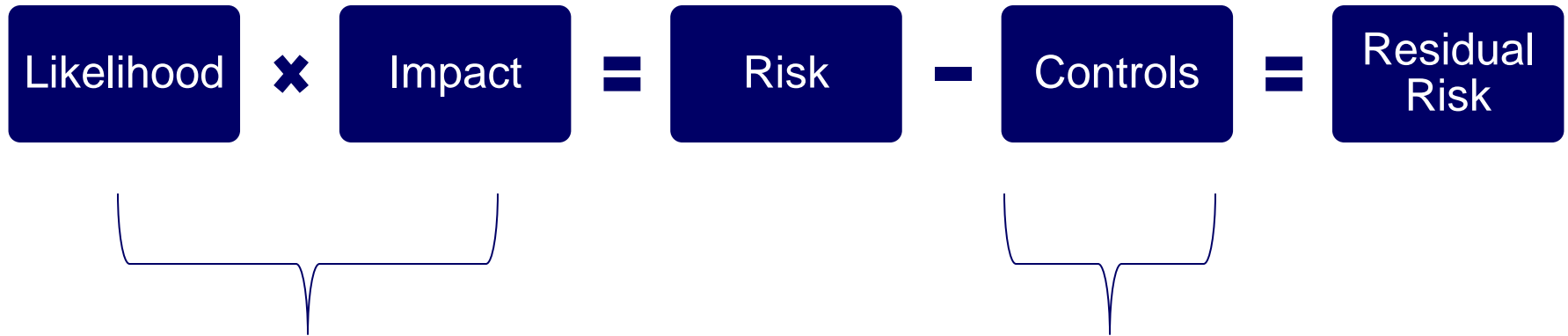
CSF Assurance Program

Simplified Risk Assessment

Overview of CSF Assurance Program

- Efficient risk assessment process
 - Referenced by Office of Civil Rights in risk assessment guidance
<http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/radraftguidance.pdf>
 - Designed to cost-effectively gather the information about security controls that is required to appropriately understand and mitigate risk
- Leverages defined, **reasonable controls** in the HITRUST Common Security Framework, the most broadly adopted security control framework in the healthcare industry
- Streamlines risk determination analysis by prioritizing areas based on analysis for breach data for the healthcare industry
- Formal and credible report for internal and external reporting
- Benchmarking data
- Recommendations for remediation

Risk Assessment Methodology (NIST, ISO)



- HITRUST Risk Areas
- Determined based upon analysis of breach data
- Significantly simplified for organizations

- HITRUST Common Security Framework
- Reasonable practice

Key Components of CSF Assurance Program

Standardized tools and processes

- Questionnaire
 - Focus assurance dollars to efficiently assess risk exposure
 - Measured approach based on risk and compliance
 - Ability to escalate assurance level based on risk
- Worksheet for reporting compliance
- Report
 - Output that is consistently interpreted across the industry

Cost effective and rigorous assurance

- Multiple assurance options based on risk
- Quality control processes to ensure consistent quality and output across CSF Assessors

High Risks for Healthcare Organizations

- Insecure and/or unauthorized removable/transportable media and laptops (internal and external movements)
- Insecure and/or unauthorized external electronic transmissions of covered information
- Insecure and/or unauthorized remote access by internal and third-party personnel
- Insider snooping and data theft
- Malicious code and inconsistent implementation and update of prevention software
- Inadequate and irregular information security awareness for the entire workforce
- Lack of consistent network isolation between internal and external domains
- Insecure and/or unauthorized implementation of wireless technology
- Lack of consistent service provider, third-party and product support for information security
- Insecure web development and applications
- Ineffective password management and protection
- Ineffective disposal of system assets

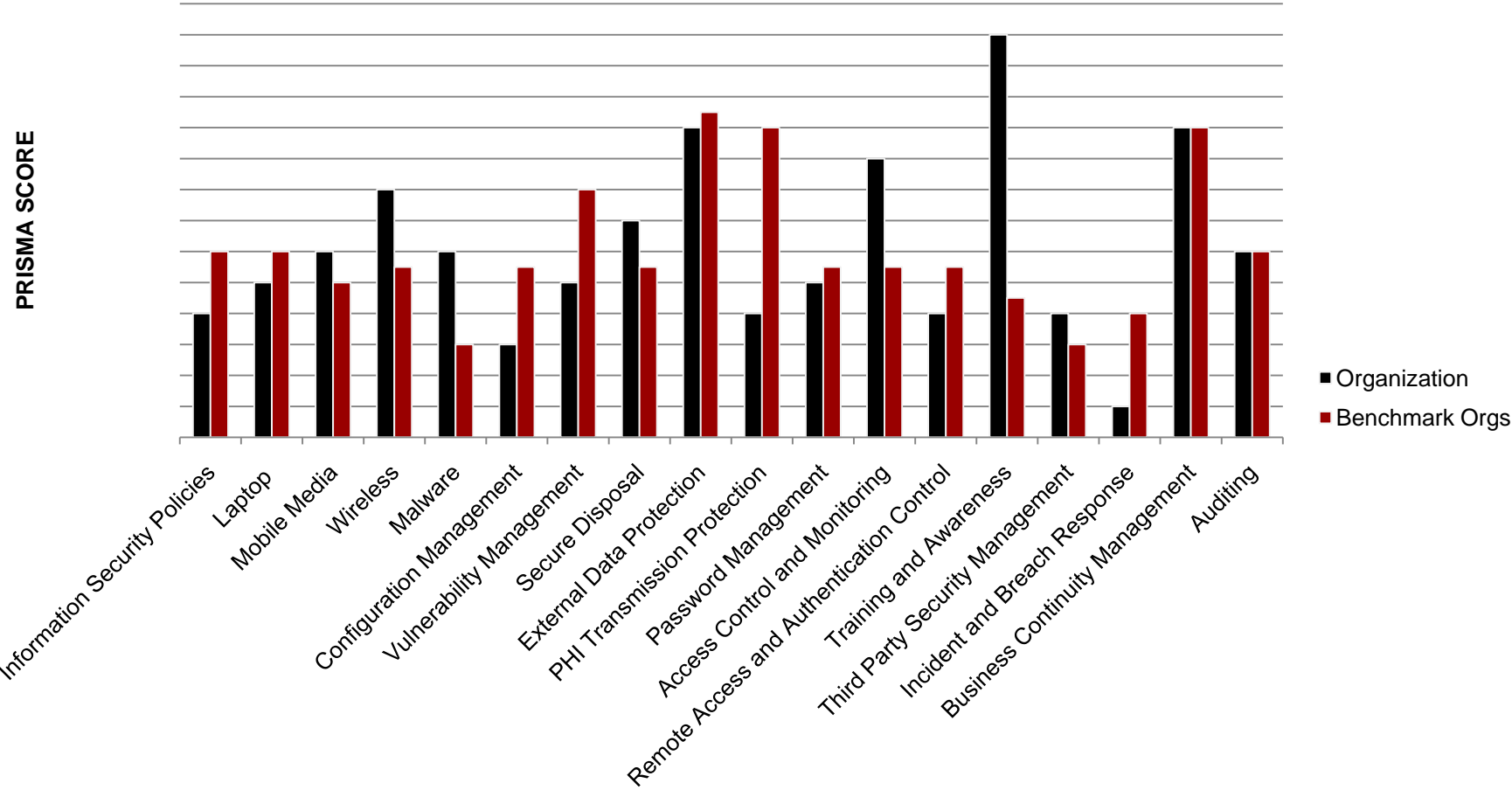
Questionnaire

Common Healthcare Information Protection (CHIP) Questionnaire:

- Innovative approach to assess the quality of information protection practices in an efficient manner
- Focus on the security capabilities and outcomes of an organization
- Leverages key measures and benchmarking
- Structured according to the high-risk areas identified in the CSF, which reflect the controls required to mitigate the most common sources of breaches for the industry

Security Capability Measures				INTRO.	SCOPE	PROFILE	PROP. METRICS
1	Information Security Policies	Answer	Comments	Measure Validation			
2	Laptop Security	Answer	Comments	Measure Validation			
CSF Cross References (click + in left margin to view)							
Number of laptops with PHI lost or stolen in the past year?							
Percentage of laptops with desktop firewall installed and operating?							
Percentage of laptops with minimum cryptographic modules operating? <i>Display more information:</i> <input type="checkbox"/>							
Document the technology tools that you use to deploy these controls:							
3	Mobile Media Security	Answer	Comments	Measure Validation			
4	Wireless Security	Answer	Comments	Measure Validation			
5	Malware Protection	Answer	Comments	Measure Validation			

Benchmark Data



HIPAA Compliance Scorecard

- Standardized output that is consistently interpreted across the industry
- HIPAA Compliance Scorecard produced for each HIPAA security requirement

HIPAA			Overall Rating
E. Administrative Safeguard (164.308)	Security Management process	(a)(1)(i) Security Policy Implementation	Overall Rating
		(a)(1)(ii)(A) Risk analysis (Required)	
		(a)(1)(ii)(B) Risk management (Required)	
		(a)(1)(ii)(C) Sanction policy (Required)	
	Workforce Security	(a)(1)(ii)(D) Information system activity review (Required)	
		(a)(3)(i) Access Control Policies and Procedures	
(a)(3)(ii)(A) Authorization and/or supervision (Addressable)			
F. Physical Safeguard (164.310)	Device and Media Controls	(a)(3)(ii)(B) Workforce clearance procedure (Addressable)	
		(a)(3)(ii)(C) Termination procedures (Addressable)	
		(d)(1) Receipt and Removal	
		(d)(2)(i) Disposal (Required)	
	Facility Access Controls	(d)(2)(ii) Media re-use (Required)	
		(d)(2)(iii) Accountability (Addressable)	
		(d)(2)(iv) Data backup and storage (Addressable)	
		(a)(1) Physical Access Policy and Procedures	
		(a)(2)(i) Contingency operations (Addressable)	
		(a)(2)(ii) Facility security plan (Addressable)	
Workstation Security	(a)(2)(iii) Access control and validation procedures (Addressable)		
Workstation Use	(a)(2)(iv) Maintenance records (Addressable)		
	(c) Physical Workstation Safeguards		
G. Technical Safeguard (164.312)	Access Control	(b) Acceptable Use Policy	
		(a)(1) Access Control Policies and Procedures	
		(a)(2)(i) Unique user identification (Required)	
		(a)(2)(ii) Emergency access procedure (Required)	
		(a)(2)(iii) Automatic logoff (Addressable)	

Assurance

Multiple assurance options:

- Self reporting
- Remote testing conducted by a CSF Assessor that includes interviews with key personnel and the review of organization charts, policies, procedures and other third-party testing that may have recently been conducted
- On-site assessment conducted by a CSF Assessor that includes remote testing and the review of system configurations and physical walk-throughs

Conducting your Meaningful Use Risk Assessment

Five steps to getting started with the CSF Assurance program:

1. Visit <http://www.hitrustalliance.net/selfassessment/> for more information on performing your meaningful use risk assessment*
2. Identify your scope
3. Perform a self assessment using the Common Healthcare Information Protection (CHIP) Questionnaire and the Compliance Worksheet**
4. Submit your CHIP to HITRUST as instructed in the questionnaire
5. Obtain a HITRUST CSF Validated Report with benchmarking data

* For other assurance options, including remote and on-site assessments via a third party CSF Assessor, please visit <http://www.hitrustalliance.net/assurance/>

** A Compliance Worksheet only needs to be completed where a compliance scorecard is required

CSF Assessors



Case Study

Background on BCHS Information Security

- Baylor Health Care System is a not-for-profit medical network that serves seven counties in the Dallas-Fort Worth metro area through more than a dozen hospitals and medical centers.
- 20,000 employees
- Baylor Health Care System (BHCS) has a dedicated department, the Office of Information Security (OIS), assigned the responsibility of information security reporting to the Chief Information Security Officer.
- Department has three groups: Information Assurance, Monitoring and Response, and Identity Management.
- All three groups consists of 22 dedicated full-time employees
- Variety of certifications including CISSP, CISA, CBLE, CBCP, CeH, GIAC, and HITRUST CSF Practitioner.

BCHS – Deployed Security Tools

- Host-based firewalls
- Workstation encryption
- Asset management and recovery
- Compliance configuration management for servers and workstations
- Wireless access point control and management
- Anti-malware
- Anti-spyware
- Inventory scanning
- Vulnerability scanning
- Web application vulnerability scanning
- Hard drive disk wiping
- Copy machine disk wiping
- Intrusion prevention system
- Enterprise class perimeter firewalls
- Web proxy
- Email gateway and encryption
- Log aggregation and correlation
- Intrusion detection system
- SFTP server
- SSL VPN
- Identity, access, and role management
- Multifactor authentication security tokens
- Remote access gateway
- Online learning tool

Steps in BCHS' Approach to Security Risk Assessment

1.

Determine Scope

Applications,
interfaces,
infrastructure

HITRUST Scoping
Template

2.

Prepare for Assessment

- Focus on high risk areas
- Identify individuals responsible for key control areas
- Conduct top down enterprise control analysis
- Do not get stuck in the weeds

-HITRUST High Risk List
-HITRUST CHIP
-HITRUST/NIST PRISMA

3.

Report

Report on findings
and remediation plan

-HITRUST CSF
Validated Report
-Corrective Action
Plan Template

4.

Track and Measure Progress

- Track progress against industry benchmarks
- Focus on measures

HITRUST CSF
Validated Report

Background on BCHS Information Security

- Interview roles:
 - Web application manager
 - Internal audit
 - Security assurance manager (risk management, business continuity management, vulnerability management, training and awareness, security policies)
 - Monitoring and response manager
 - Server engineering
 - Desktop engineering
 - Human resources
 - Access and identity management
 - Application developer

Background on BCHS Information Security

- Documents review:
 - Asset inventory with risk classification
 - Network diagram
 - Organization chart
 - Business Associate Agreement template
 - Risk assessment program
 - Application assessment questionnaires
 - Sample web application assessments
 - Sample network vulnerability assessments
 - Sample attack and penetration report
 - Project/engagement hierarchy

Background on BCHS Information Security

- Documents review (continued):
 - Business continuity management program
 - Business Impact Analysis templates
 - Business continuity plan template
 - Disaster recovery plan template
 - Sample business continuity and disaster recovery plans
 - Sample security awareness and training materials
 - Policies and standards framework
 - Policy and standards third party review report
 - Incident monitoring and response program and associated procedures
 - Security council charter

Lessons Learned

- Healthcare providers have challenges – you will have gaps
- Assessment methodology
 - Sound NIST based approach
 - Very efficient approach
- Credibility with executives and regulators
- Positions us well for meaningful use but also helps us address longer term goals and maintain HIPAA compliance

For More Information:

For more information on the CSF Assurance Program visit:

www.HITRUSTAlliance.net/assurance

For a list of HITRUST CSF Assessors visit:

www.hitrustalliance.net/Assessors_List.pdf

For assistance, contact:

info@HITRUSTalliance.net