



HITRUST Key Programs and Services 2015

Securing the Future of the Healthcare Industry

Contents

About HITRUST	3
HITRUST in a Snapshot	4
HITRUST Key Focus Areas	5
Risk Management and Compliance	6
Risk Management	8
Cybersecurity	9
Education	10
Thought Leadership	11
Papers and Presentations	11
Sponsored Industry Working Groups	12
In the Media	13
Governmental Affairs	16
Key Accomplishments	18
HITRUST Board of Directors	19
Management Team	20
Footnotes	23

About HITRUST

Founded in 2007, the Health Information Trust Alliance (HITRUST) was born out of the belief that information protection should be a core pillar of, rather than an obstacle to, the broad adoption of health information systems and exchanges. HITRUST, in collaboration with public and private healthcare technology, privacy and information security leaders, has championed programs instrumental in safeguarding health information systems and exchanges while ensuring consumer confidence in their use.

HITRUST programs include the establishment of a common risk and compliance management framework (CSF); an assessment and assurance methodology; educational and career development; advocacy and awareness; and a federally recognized cyber Information Sharing and Analysis Organization (ISAO) and supporting initiatives.

More Info: <https://hitrustalliance.net/>

HITRUST in a Snapshot

Best known for:

- Development of HITRUST CSF—now in its seventh major release
- Cyber preparedness and response exercises—CyberRX

CSF Adoption:

- By 83 percent of hospitals¹ (most widely adopted)
- By 82 percent of health plans² (most widely adopted)

CSF Assurance Adoption:

- Over 23,000 CSF assessments in last three years (10,000 in 2014)
- Most widely utilized approach by healthcare organizations and third party risk assessments
- Supports State of Texas Privacy and Security Certification (<http://hitrustalliance.net/texas/>)

Most Active Cyber Center in Health Industry - Cyber Threat Intelligence and Incident Coordination Center

- Information sharing agreement with Department of Health and Human Services (HHS) and Department of Homeland Security (DHS)
- Industry-specific cyber threat intelligence and industry incident coordination—“community defense”
- Partnership with HHS for monthly industry cyber threat briefings (<http://hitrustalliance.net/cyber-threat-briefings/>)
- Partnership with HHS for industry cyber threat preparedness exercises – CyberRX (<http://hitrustalliance.net/cyberrx/>)
- Cyber Threat Exchange (CTX) as industry cyber threat early warning system and to automate indicator of compromise (IOC) distribution (<https://hitrustalliance.net/cyber-threat-xchange/>)

Information Protection Education and Training

- Over 1300 professionals obtained Certified Common Security Framework Practitioner (CCSFP) designation—CSF specific
- Partnered with International Information System Security Certification Consortium, Inc., (ISC)²® to develop broader healthcare certified information security professional credentia—HealthCare Information Security and Privacy Practitioner (HCISPP)
- Annual conference: In 2012 HITRUST began holding health information protection professional annual conference
- Partnered with Southern Methodist University for healthcare CISO fellowship program

HITRUST Key Focus Areas

Management and Compliance

- CSF
- CSF Assurance
- MyCSF

Cybersecurity

- Threat Intelligence and Incident Coordination Center
- Cyber Threat XChange
- CyberRX
- Cyber Threat Briefings
- Cyber Discovery Study

Education

- HITRUST Academy
- Annual HITRUST Conference
- Leadership Roundtable
- Educational Webinar Series

Thought Leadership

- White Papers
- Research Initiatives
- In the Media



Risk Management and Compliance

The CSF – Built for Healthcare

HITRUST, in collaboration with healthcare, business, technology and information security leaders, has established the HITRUST CSF, a certifiable framework that can be used by any and all organizations that create, access, store or exchange personal health and financial information.

When developing the HITRUST CSF, HITRUST recognized the global nature of healthcare and the need to gain assurances around the protection of covered information from non-U.S. business associates, which led to ISO/IEC 27001 being used as the foundation upon which the CSF controls were built. ISO/IEC 27001 provides an international standard for the implementation and maintenance of an information security management system (ISMS) with high-level controls designed to suit almost any organization in any industry in any country.

The HITRUST CSF provides coverage across multiple healthcare specific standards and includes significant components from other well-respected IT security standards bodies and governance sources. The HITRUST CSF addresses industry challenges by leveraging and enhancing existing standards and regulations to provide organizations of varying sizes and risk profiles with prescriptive implementation requirements.

Standards Incorporated Into the CSF

- HIPAA: Security, Breach, and Privacy Rules
- ISO/IEC 27001, 27002, 27799
- CFR Part 11
- COBIT 4.1, COBIT 5
- NIST SP 800-53 Revision 4
- NIST SP 800-66
- NIST Cyber Security Framework
- PCI DSS version 3
- FTC Red Flags Rule
- JCAHO IM
- 201 CMR 17.00 (State of Mass.)
- NRS 603A (State of Nev.)
- CSA Cloud Controls Matrix v1
- HHS Secretary Guidance
- CMS IS ARS
- MARS-E v1
- IRS 1075
- Texas Health and Safety Code (THSC) 181
- Title 1 Texas Administrative Code (TAC) 390.2

Risk Management and Compliance

The CSF – Built for Healthcare

HITRUST maintains the relevancy of the CSF by regularly reviewing changes in source frameworks and best practices due to changes in the regulatory or threat environment, as well as breach incidents are analyzed to determine the root cause and impact to the CSF. The CSF is updated no less frequently than annually. Other standards and governments regulation, such as updates to ISO/IEC 27001 and NIST SP 800-53, are made much less frequently and may not necessarily reflect new federal (e.g., HITECH) or state regulations. The ongoing enhancements and maintenance to the CSF provide continuing value to healthcare organizations, sparing them from much of the complexity and expense of integrating and tailoring these multiple requirements and best practices into a custom framework of their own. As a result, the CSF has seen very broad adoption in the industry.

Comparison of HITRUST, ISO & NIST

Factor ¹	ISO/IEC 27001	NIST SP 800-53	HITRUST CSF
ISO 27001-Based	✓	✗	✓
Integrated Compliance Framework	✗	✗	✓
Healthcare Specific	✗ ²	✗ ²	✓ ³
Healthcare Standard	✗	✗ ⁴	✓
Prescriptive	✗ ⁵	✓	✓
Controlled Scaling	✗	✗	✓ ⁶
Controlled Tailoring	✗	✓ ⁷	✓
Control Compliance-Based	✗ ⁸	✓	✓
Organizational Certification	✗	✓	✓
Supports Third-Party Assurance	✓	✗	✓
Assessment Guidance	✗ ⁹	✓	✓
Tool Support	✗	✓	✓

Table 1: Why the CSF is well accepted in the industry

Risk Management

CSF Assurance & MyCSF

MyCSF: A full-featured, user-friendly, integrated and managed tool that streamlines the entire information compliance & risk management process from policy, assessment & remediation to incident & exception management.

More Info: <https://hitrustalliance.net/mycsf/>

CSF Assurance Reports: The CSF Assurance program includes the risk management oversight and assessment methodology governed by HITRUST and designed for the unique regulatory and business needs of the healthcare industry. The HITRUST CSF Assurance Program delivers simplified compliance assessment and reporting for HIPAA, HITECH, state and business associate requirements. Leveraging the HITRUST (CSF) organizations can streamline the compliance process & reduce costs with a standardized approach to performing assessments & reporting security controls by utilizing the HITRUST CSF Assurance Program.

More Info: <https://hitrustalliance.net/csf-assurance/>

Texas Covered Entity Privacy and Security Certification Program: HITRUST and Texas Health Services Authority (THSA) have partnered to develop and implement the Texas Covered Entity Privacy and Security Certification Program, the first state recognized certification of its kind. It is a certification that Texas covered entities can introduce in an action or proceeding imposing an administrative penalty or assessing a civil penalty related to an unauthorized disclosure.

More Info: <https://hitrustalliance.net/texas/>

Combined CSF and SOC2 Reports: HITRUST and the American Institute of CPAs (AICPA) have partnered to enable organizations to utilize the HITRUST CSF as the controls for their SSAE16 SOC2. A converged HITRUST and AICPA reporting model helps organizations leverage the work invested in a CSF implementation to meet their Service Organization Control (SOC2) reporting requirements.

More Info: <https://hitrustalliance.net/soc2/>

Cybersecurity

HITRUST Cyber Threat Intelligence and Incident Coordination Center: The Cyber Threat Intelligence and Incident Coordination Center provides cyber threat warning and threat intelligence services to help healthcare organizations prioritize their cybersecurity efforts and raise security awareness by informing them of general and sector-specific threats impacting the industry. This advanced level of healthcare-specific knowledge allows an organization to distill the noise of wider threats and focus on potential targeted threats.

Cyber Threat XChange (CTX): The HITRUST Cyber Threat XChange (CTX) automates the process of collecting and analyzing cyber threats and distributing actionable indicators in electronically consumable format that organizations of varying sizes and cyber security maturity can utilize to improve their cyber defenses.

More Info: <https://hitrustalliance.net/cyber-threat-xchange/>

Cyber Threat Briefings: As the number of cyber-attacks targeted at the healthcare industry rises, HITRUST is partnering with the U.S. Department of Health and Human Services to conduct monthly cyber threat briefings to aid organizations in better understanding current and probable cyber threats relevant to the healthcare industry and to share best practices for cyber threat defense and response.

More Info: <https://hitrustalliance.net/cyber-threat-briefings/>

CyberRX: CyberRX is a series of no cost, industry-wide exercises coordinated by HITRUST in conjunction with the U.S. Department of Health and Human Services, with the mission to mobilize healthcare organizations and explore innovative ways of improving preparedness and response against cyber attacks intended to disrupt the nation's healthcare operations.

More Info: <https://hitrustalliance.net/cyberrx/>

Cyber Discovery Study: HITRUST is undertaking the first empirical and comprehensive study to analyze the methods, severity and pervasiveness of cyber threats targeting a variety of healthcare organizations. The study will enable a better understanding of the actual magnitude, complexity, relations of cyber-attacks, commonalities of target organizations and data, and degree of cyber threats persisting within organizations. The goal is to accurately identify attack patterns and persistence, as well as the magnitude and sophistication of specific threats across enterprises.

More Info: <https://hitrustalliance.net/cyber-discovery/>

Education

HITRUST Academy: HITRUST Academy offers the only training courses designed to educate healthcare security professionals about information protection in the healthcare industry and the utilization of the HITRUST CSF to manage risk. The courses are intended to prepare security professionals for assessing against the evolving compliance landscape shaped by Omnibus, HIPAA, CMS and various other federal, state and business requirements.

More Info: <https://hitrustalliance.net/hitrust-academy/>

Annual HITRUST Conference: The HITRUST Conference is the only event dedicated to exploring all aspects of healthcare information protection and utilization of the HITRUST CSF and CSF Assurance Program; with the goal of enabling attendees to more effectively meet compliance requirements and improve information protection.

More Info: <https://hitrustalliance.net/hitrust2015/>

Leadership Roundtable: This program is intended exclusively for executives responsible for the protection of healthcare information and for the purpose of exploring, discussing, learning, collaborating and, where appropriate, agreeing upon a variety of topics relating to information security in the healthcare industry.

More Info: <https://hitrustalliance.net/leadership-roundtable/>

Educational Webinar Series: Best Practices & Lessons Learned Implementing the CSF– Webinar series that featured real world examples from organizations using the HITRUST CSF and CSF Assurance Program to manage their information security programs. Hear from a diverse group of presenters covering best practices, lessons learned and practical information that can be leveraged by other organizations facing the same requirements and challenges.

More Info: <https://hitrustalliance.net/webinars/>

Thought Leadership

Papers and Presentations

HITRUST brings its years of experience and expertise to the development of papers and presentations for use by the industry in protecting healthcare information.

Sample documents include:

- **How to Approach/Simplify Meaningful Use Security and Privacy Risk Assessments (2010-2012)**
https://hitrustalliance.net/content/uploads/2014/05/HITRUST-CSF-Assurance-Program-Meaningful-Use-Webinar_Final.pdf
https://hitrustalliance.net/content/uploads/2014/05/IMU-Security_Risk-Assessments-SecureWorld.pdf
- **Texas House Bill 300 Compliance (2012)**
<https://hitrustalliance.net/content/uploads/2014/05/Texas-House-Bill-300-Compliance-through-HITRUSTv1.2.1.pdf>
- **Leveraging Healthcare's Risk Management Framework to Manage Business Risk (2013)**
https://hitrustalliance.net/content/uploads/2014/07/Managing_Business_Risk_with_HITRUST_Webinar.pdf
- **Streamlining and Enhancing the NIST Framework to Achieve HIPAA Compliance (2013)**
<https://hitrustalliance.net/hitrust-csf-streamlines-enhances-nist-achieve-hipaa-compliance/>
<https://hitrustalliance.net/content/uploads/2014/05/HITRUST-RMF-Whitepaper.pdf>
- **Guidance for Healthcare Organizations to Assess Cybersecurity Preparedness (2013-2014)**
<https://hitrustalliance.net/content/uploads/2014/06/HiTrustCSFCybersecurityTable.pdf>
- **Risk Analysis Guidance (2013-2014)**
<https://hitrustalliance.net/content/uploads/2014/10/RiskAnalysisGuide.pdf>
- **Using a Healthcare Cybersecurity Framework to Support a State-level Covered Entity Certification Program (2014)**
<https://hitrustalliance.net/content/uploads/2014/05/HITRUST-RMF-and-Texas-Certification-A-Model-for-Industry-v1.pdf>
- **Implementing the NIST Cybersecurity Framework in Healthcare (2014)**
<https://hitrustalliance.net/content/uploads/2014/06/ImplementingNISTCybersecurityWhitepaper.pdf>
<https://hitrustalliance.net/nist-csf-webinar/>
- **Risk vs. Compliance-based Information Protection (2014)**
<https://hitrustalliance.net/content/uploads/2014/06/RiskVsComplianceWhitepaper.pdf>
- **Why your HIPAA Risk Analysis May Not Actually Be HIPAA Compliant (2014)**
<https://hitrustalliance.net/content/uploads/2014/05/Why-your-HIPAA-risk-analysis-may-not-actually-be-HIPAA-compliant-v1.pdf>

Thought Leadership

Sponsored Industry Working Groups

HITRUST has been a leader in identifying and tackling the developing information security and privacy challenges in the healthcare space. Through its sponsorship of numerous working groups, HITRUST has been a positive influence in closing identified gaps in the field.

- Steering Committee; Health Information Systems and Medical Devices Security Working Group (2015-Present)
- Industry Advisory Panel; AICPA SOC2 Working Group (2014-Present)
- CSF Risk Factors Working Group (2014-Present)
- Cyber Threat Working Group (2014-Present)
- Cybersecurity Working Group (2013-2014)
- De-identification Working Group (2013-Present)
- Privacy Integration Working Group (2013-2014)
- Content Definition Development Working Group (2011)
- Mobile Devices Working Group (2011)
- Cloud Security Working Group (2011)
- Health Information Exchange Working Group (2011)

Thought Leadership

In the Media

HITRUST is recognized in the healthcare and cybersecurity communities as a thought leader and is often featured in the news and sought out for expert comment. Recent examples in the media include:

- ***HITRUST Updates Cybersecurity Approach, HealthITSecurity*** (2/10/2015)
<http://healthitsecurity.com/2015/02/10/hitrust-updates-healthcare-cybersecurity-approach/>
- ***HITRUST Helps Anthem, Others in Initial Hack Investigation, Insurance Networking News*** (2/6/2015)
http://www.insurancenetworking.com/news/risk_management/HITRUST-Helps-Anthem-Others-in-Initial-Hack-Investigation-35505-1.html#Login
- ***3 Key Data Security Issues HITRUST Needs to Consider, Healthcare Dive*** (1/22/2015)
<http://www.healthcaredive.com/news/3-key-data-security-issues-hitrust-needs-to-consider/355112/>
- ***HITRUST Likes Obama's Cyber Pivot, Politico*** (1/22/2015)
<http://www.politico.com/morninghealth/0115/morninghealth16821.html>
- ***HITRUST Establishes Healthcare Security Working Group, Infosecurity Magazine*** (1/15/2015)
<http://www.infosecurity-magazine.com/news/hitrust-healthcare-security-group/>
- ***HITRUST Adds Privacy Controls to Framework, HealthInfoSecurity*** (1/12/2015)
<http://www.healthcareinfosecurity.com/hitrust-adds-privacy-controls-to-framework-a-7772>
- ***Reboot 25: The Influencers, SC Magazine*** (12/2014)
<http://www.scmagazine.com/top-influencers-in-information-security/article/385069/2/>

Thought Leadership

In the Media

- **Acting Out: Cyber Simulation Exercises** (11/3/2014)
<http://www.scmagazine.com/acting-out-cyber-simulation-exercises/article/377716/>
- **HITRUST Offers Automated Early Warning on Cyber Threats, Healthcare Informatics** (10/18/2014)
<http://www.healthcare-informatics.com/article/hitrust-offers-automated-early-warning-cyber-threats>
- **Community Health Breach Highlights Healthcare Security Vulnerabilities, CIO** (8/25/2014)
<http://www.cio.com/article/2597970/healthcare/community-health-breach-highlights-healthcare-security-vulnerabilities.html>
- **750 Organizations Want In on CyberRX Attack Simulations, FierceHealthIT** (9/24/2014)
<http://www.fiercehealthit.com/story/750-organizations-want-cyberrx-attack-simulations/2014-09-04>
- **Industry Working to Support CSF Alignment with AICPA's SOC 2 Reporting** (6/9/2014)
<https://hitrustalliance.net/industry-working-support-csf-alignment-aicpas-soc-2-reporting/>
- **Attack Exercise Reveals Threat-sharing Roadblock Within Health Orgs, SC Magazine** (4/21/2014)
<http://www.scmagazine.com/attack-exercise-reveals-threat-sharing-roadblock-within-health-orgs/article/343566/>
- **How Texas is Boosting HIPAA Compliance** (4/30/2014)
<https://hitrustalliance.net/texas-boosting-hipaa-compliance/>
- **Simulated Cyber Attack Finds Gaps in Preparedness, GovHealthIT** (4/22/2014)
<http://www.govhealthit.com/news/simulated-healthcare-cyber-attack-shows-gaps-security>

Thought Leadership

In the Media

- **Health Insurers, CVS To Require Security Tests of Business Associates, *ihealthbeat*** (5/9/2013)
<http://www.ihealthbeat.org/articles/2013/5/9/health-insurers-cvs-to-require-security-tests-of-business-associates.aspx>
- **HHS, HITRUST Offer Free Cyberthreat Briefings, *ModernHealth4are*** (3/14/2014)
<http://www.modernhealthcare.com/article/20140314/NEWS/303149904>
- **HITRUST Forms Working Group to Develop Information Sharing Framework for Healthcare Sector, *SecurityWeek*** (2/30/2013)
<http://www.securityweek.com/hitrust-forms-working-group-develop-information-sharing-framework-healthcare-sector?>
- **HITRUST Position on the NIST Cybersecurity Framework** (2/13/2014)
<https://hitrustalliance.net/hitrust-position-nist-cybersecurity-framework/>
- **HITRUST CSF Streamlines and Enhances NIST to Achieve HIPAA Compliance** (2014)
<https://hitrustalliance.net/hitrust-csf-streamlines-enhances-nist-achieve-hipaa-compliance/>

Governmental Affairs

HITRUST has been engaged heavily in the health security and IT debate in Washington. Specifically, HITRUST has engaged federal agencies and Congress in a sustained dialog about: information sharing, the CSF, healthcare security and related policies. We have been actively meeting with congressional leaders to propose solutions to legislative language on cybersecurity and work with agencies to shape executive branch initiatives regarding information sharing.

Cybersecurity Legislation: President Obama introduced several new cybersecurity legislative proposals. Congress is likely to take up legislation to promote the sharing of cyber threat information between the public and private sector in the near future. The role of Information Sharing and Analysis Organizations (ISAOs) are to be a large part of the debate. HITRUST has been leveraging its position as healthcare industry's leading ISAO. HITRUST has engage directly with members and staff of the House and Senate Intelligence, Homeland Security and Healthcare related committees as well as members and staff of the House and Senate that have shown leadership on healthcare related cybersecurity and privacy. HITRUST has been meeting directly with members and staff to influence hearings as Congress considers the various cybersecurity and privacy related proposals and is working with the Senate Intelligence Committee and the House Homeland Security Committee on draft language.

Recently, Dan Nutkis, HITRUST CEO, testified at a House of Representatives Committee hearing sharing his viewpoints on the evolving nature of cybersecurity threats facing the private sector. Additionally, HITRUST is frequently asked by congressional committees to weigh in on cybersecurity policy matters related to healthcare.

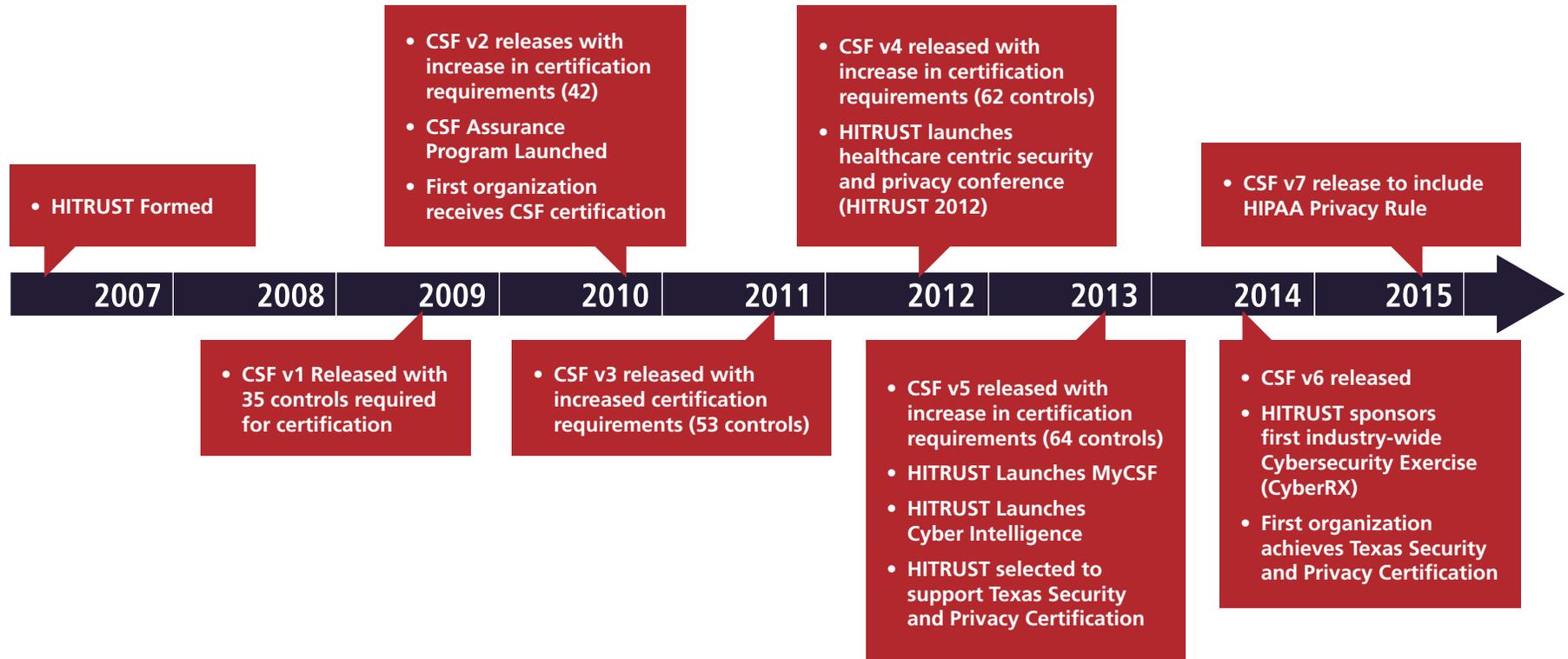
Data Breach and Privacy: The current regulatory framework in the United States does not provide a national uniform data breach notification standard that applies to all personally sensitive information. The President has introduced several new cybersecurity legislative proposals, including one to establish a national data security and data breach standard and a national 30 day breach notification rule. Currently, the proposals are exempting HIPAA covered entities and health related information. HITRUST continues to fully engage with policy makers on behalf of the healthcare industry and as a leader in security and data lost prevention as well as privacy protections.

Governmental Affairs

Information Sharing: Ensuring the protection and resilience of the nation's critical infrastructure is a shared responsibility among multiple stakeholders. Public-private partnerships are the foundation for effective critical infrastructure protection and resilience strategies, and that timely, trusted information sharing among stakeholders is essential to the security of the nation's critical infrastructure. HITRUST, continues to work with policy makers to ensure that ISAOs play a vital role in further developing the private sector information sharing and partnering with government. HITRUST continue to work closely with FBI, DHS, HHS and NIST to optimize information sharing and incident responses.

Additional Priorities: Ensuring HITRUST continues to develop ways to engage with the Office for Civil Rights (OCR) and policy makers to ensure that OCR is effectively conducting audits and security assessments to position stakeholders to discuss frameworks, best practices, trends and safe harbor potential. HITRUST continues to directly engage with the Administration such as Secretary Burwell, Office of the National Coordinator on Health IT security proposals. (<https://hitrustalliance.net/letter-from-hitrust-ceo-to-secretary-burwell/>)

Key Accomplishments



HITRUST Board of Directors

HITRUST is led by a seasoned management team and governed by a Board of Directors made up of leaders from across the healthcare industry and its supporters. These leaders represent the governance of the organization, but other founders also comprise the leadership to ensure the framework meets the short and long term needs of the entire industry.



Daniel Nutkis
Chief Executive Officer
HITRUST



Kimberly Gray, Esq., CIPP
Chief Privacy Officer, Global
IMS Health



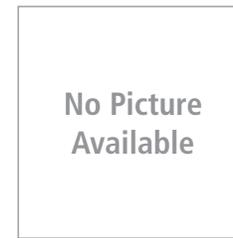
Erick Rudiak
Information Security Officer
Express Scripts, Inc.



Pamela Arora
Senior Vice President
& Chief Information Officer
Children's Medical Center



Omar Khawaja
Vice President &
Chief Information
Security Officer
Highmark Inc.



Michael Wilson
Vice President & Chief
Information Security Officer
McKesson Corporation



Ray Biondo
Divisional Senior
Vice President & Chief
Information Security Officer
Health Care
Service Corporation



**Roy R. Mellinger,
CISSP-ISSAP, ISSMP, CIM**
Vice President, IT Security
& Chief Information
Security Officer
Anthem, Inc.



Robert E. Booker
Chief Information
Security Officer
UnitedHealth Group



Jon Moore
Chief Information
Security Officer
Humana Inc.

Management Team



Daniel Nutkis – Chief Executive Officer

Daniel Nutkis is the founder and Chief Executive Officer for HITRUST. Mr. Nutkis has more than 20 years of experience in providing strategic advisory services in areas relating to health information technology. His recent focus has been on technologies that enable information protection and strategic business objectives. Prior to founding HITRUST, he held various positions with email encryption and e-prescribing service company Zix Corporation (NASDAQ: ZIXI), including Executive Vice President, Strategy, and President, Care Delivery. He was also with Ernst & Young LLP's healthcare emerging technology groups as National Director. He has led a number of industry research activities on eHealth vulnerabilities and has been a founding member of work groups and accreditations such as WEDI, CPRI and HISPP.

Dan has also been recently recognized as a *top information security influencer in 2014 by SC Magazine*, and in *2015 by Health Information Security Magazine*.



Michael Frederick – Vice President, Assurance Services and Product Development

Michael Frederick has 20+ years' experience in information security. He is currently the Vice President of Assurance Services and Product Development at HITRUST. Prior to joining HITRUST he was CEO of The Frederick Group, a professional services firm focused on security risk management in healthcare. He served as Chief Information Security Officer (CISO) for eight years at a large healthcare system. While in this role, he led the organization in becoming the first hospital system to be certified under the HITRUST CSF and was the industry lead in the provider space during the development of the CSF. He has been a speaker at numerous security events and has been published on the topics of risk management, applying security practices within an organization, and how to build an effective security organization. Prior to his CISO role, he was a security architect, security manager in industry and a security consultant in various large accounting firms. He has been a Certified Information System Security Professional (CISSP) since 1999.

Management Team



Steven Penn – Senior Director, CSF Development and Education Program

Steve Penn is an experienced security professional with 15+ years of information security experience. He currently serves as the Senior Director for HITRUST Cyber Security Framework Development and Education. His varied background includes experience in the Public and Private sector leading and supporting information security for Healthcare, Law Enforcement, Infrastructure, and Defense. He has a Master's Degree in Information Assurance from Norwich University and currently holds the following ISC2 Certifications; CISSP, ISSMP, ISSAP, CAP, HCISPP. Additionally he has volunteered with ISC2 for the past seven years as a subject matter expert and content developer for the CISSP, ISSMP, CAP, and HCISPP exams.



Ken Vander Wal – Chief Compliance Officer

Ken Vander Wal's role as Chief Compliance Officer at HITRUST involves providing supervision and oversight to the HITRUST CSF Assurance program. In this capacity, he is responsible for ensuring the quality, completeness and adequacy of the work performed by CSF Assessor organizations. Mr. Vander Wal joined HITRUST after retiring from Ernst & Young where he was a partner in the Technology and Security Risk Services (TSRS) practice and responsible for its global TSRS quality and risk management program. With almost 40 years of IT experience, he has experience in a variety of industries in multiple areas of information systems, including systems development, systems programming, project management, quality assurance, IT auditing and systems security. As the national leader of TSRS quality, Mr. Vander Wal was responsible for ensuring quality was an integral component of Ernst & Young's methodologies, engagement staffing and service delivery. In this role as well as his previous roles, he served major clients as the IT audit engagement partner or as the quality assurance partner. Mr. Vander Wal is a member of the American Institute of Certified Public Accountants and the Information Systems Audit and Control Association. He is both a Certified Public Accountant and a Certified Information Systems Auditor.

Management Team



Bryan Cline, PhD – Senior Advisor

Bryan Cline is a Senior Advisor to the Health Information Trust Alliance (HITRUST) and provides thought leadership for the continuing development and implementation of the HITRUST risk management framework and its various components. Previously the VP of CSF Development and Implementation, Dr. Cline helped mature the HITRUST CSF and CSF Assurance Program into a more comprehensive risk management framework that is a model implementation of the national Framework for Critical Infrastructure Cybersecurity for healthcare; spearheaded development of the Texas Covered Entity Privacy and Security Certification program; and partnered with (ISC)² to create the Health Care Information Security and Privacy Practitioner (HCISPP) credential. Dr. Cline also served as the Chief Information Security Officer (CISO) and Director of Information Security at Catholic Health East, and as the CISO and Director of Information Security Risk Management at The Children’s Hospital of Philadelphia. Bryan holds a Doctorate in information systems with a concentration in information assurance policy from the University of Fairfax, a Master of Science degree in industrial engineering with a concentration in operations research from the University of Oklahoma, and a Baccalaureate in mathematics from the University of Texas at Arlington. Dr. Cline also serves as an adjunct professor and dissertation advisor for the University of Fairfax and holds the CISSP-ISSEP, CISM, CISA, ASEP, CCSFP, and HCISPP credentials.

Footnotes

HITRUST in a Snapshot

1. Based on facilities in the 2011 AHA hospital and health system data as of Dec 2014
2. Based on health plans with over 500,000 members as of Dec 2014

Risk Management and Compliance—Comparisons of HITRUST, ISO & NIST

1. Factor Definitions:
 - a. ISO 27001-Based: Is the framework based on the international standard?
 - b. Integrated Compliance Framework: Have multiple regulatory, standards, frameworks and best practices been incorporated into the framework?
 - c. Healthcare Specific: Was the framework designed to accommodate the specific, unique needs of the healthcare industry?
 - d. Healthcare Standard: Does the framework have significant adoption within the industry?
 - e. Prescriptive: Are the framework control requirements sufficiently detailed to reduce ambiguity in implementation?
 - f. Controlled Scaling: Can the framework be scaled to the specific needs of a healthcare organization in a centralized, pre-defined way?
 - g. Controlled Tailoring: Does the framework allow the replacement of specified controls with alternate controls in a centralized, pre-defined way?
 - h. Control Compliance-Based: Is risk determined through a gap-analysis of the control requirements and the maturity with which they're implemented?
 - i. Organizational Certification: Does the framework provide for formal certification of the state of control compliance within an organization?
 - j. Supports Third Party Assurance: Does the framework provide an adequate mechanism for the sharing of reasonably accurate and consistent risk information amongst organizations?
 - k. Assessment Guidance: Does the framework provide prescriptive guidance on how controls should be assessed through documentation reviews, observation, interviews or testing?
 - l. Tool Support: Availability of specific tools organizations may use to assess and manage controls and risks to the organization.
2. Additional guidance for healthcare is provided separately (ISO/IEC 27799 & NIST SP 800-66)
3. HITRUST is rapidly becoming the de facto standard for the healthcare industry
4. NIST and OCR collaborate on specific tools like the HSR Toolkit but do not promulgate NIST SP800-66 as an industry standard for healthcare
5. ISO 27001 provides relatively general requirements compared to NIST and HITRUST
6. Only HITRUST scales control requirements based on organizational, system and regulatory risk factors7 ISO compliance
7. Only HITRUST provides a formal, central review and approval process for alternative controls
8. ISO compliance is based primarily on an evaluation of the ISMS rather than on a gap analysis of the controls and subsequent risk to the organization
9. CSF Assessor organizations are not required to use the general guidance provided in ISO/IEC 27008



855.HITRUST
(855.448.7878)
www.HITRUSTalliance.net