ecfirst | Perfecting the Art of *Active* Cyber Defense

HITRUST CSF Certification = *Credible* HIPAA Compliance Program

Exec Brief

Entities have been fined in millions for lack of a credible HIPAA compliance program. HIPAA compliance in 2018 is at least a seven-figure risk to covered entities and business associates. A key question facing organizations is how does it establish a credible HIPAA compliance program? This is where HITRUST CSF certification emerges as an area of executive importance – it directly addresses HIPAA and HITECH compliance, as well as other mandates such as the European Union (EU) General Data Protection Regulation (GDPR), NIST CsF, as well as state cybersecurity regulations such as New York State Cybersecurity Requirements for Financial Services Companies (23 NY CRR 500).

The focus of this brief is to examine how HITRUST CSF Certification = *Credible* HIPAA Compliance!

Content

Uday Ali Pabrai
Cyber Security & Compliance Expert

Senior leadership must ensure that the organization has an enterprise-wide HIPAA compliance program – a program that continually addresses HIPAA mandates. The HITRUST CSF standard is prescriptive, flexible, and comprehensive – it can be used by organizations small or large, business associate or covered entity, to address HIPAA compliance requirements, and more.

Senior leadership must have the confidence that HIPAA non-compliance is not a risk to the organization; that the organization is continually HIPAA compliant, and can demonstrate the same.

The HIPAA settlements, fines, and Corrective Action Plans (CAP) from 2008 through 2018 provide a clear directive to the healthcare industry, including business associates – establish a credible, evidence-based HIPAA compliance program. HITRUST CSF certification provides this confidence to senior executives about the state of its HIPAA compliance program.

Why the HITRUST CSF for HIPAA Compliance?

The HITRUST CSF provides a comprehensive, scalable, and a technology-neutral framework to address HIPAA mandates. It is a formal and formidable framework, developed specifically for the healthcare industry, to address privacy and security regulatory requirements. We know compliance with HIPAA requires an organization to address the following on a continual basis:

- HIPAA Privacy Rule
- HIPAA Security Rule
- HITECH Breach Notification

Everything in the HIPAA and HITECH regulations comes down to these three words: “reasonable and appropriate.” This implies the organization must implement “reasonable and appropriate” safeguards to secure all enterprise ePHI.

The HITRUST CSF enables an organization, be it a covered entity or a business associate, to formally address these HIPAA mandates. With the application of the HITRUST CSF, an organization knows the exact gaps to address to help ensure credible HIPAA compliance.

HIPAA Safeguards Map to HITRUST CSF Control Categories/Domains

The pillars of HIPAA compliance are based on defined safeguards (e.g. Administrative, Physical, Technical and others), as well as Standards and Implementation Specifications. The HITRUST CSF is architected on the ISO/IEC 27001:2005 control clauses. All HIPAA requirements are mapped by the HITRUST CSF to Control Categories/Domains. The CSF is comprised of:

- 14 Security Control Categories
- 45 Control Objectives
- 149 Control Specifications

Control Categories/Domains include Access Control, Security Policy, Business Continuity Management, Privacy Practices and more. Each control domain consists of one or more control objectives; a control may have up to three levels of implementation requirements. These may include requirements integrated from several sources and standards such as HIPAA, PCI DSS, and NIST.

Why are these control domains relevant for HIPAA compliance? These control domains in HITRUST map back and address all HIPAA-related Standards and associated Implementation Specifications. For example, the Sanctions Policy Implementation Specification in the HIPAA Security Rule maps to Disciplinary Process in the HITRUST CSF v9.1.

The HITRUST CSF establishes maturity levels relevant to evaluating an organization's compliance and security program. There are five formally defined maturity levels:

1. Policy
2. Procedures
3. Implemented
4. Measured
5. Managed

By basing an organization's HIPAA compliance program on the HITRUST CSF, we can determine, in a structured way, how compliance requirements are being addressed for each of the defined HIPAA requirements. Have policies been developed? Are procedures practiced? Which controls have been implemented? What are the control deficiencies? How are the controls monitored and managed?

The HITRUST CSF defines the compliance scale maturity levels as:

- Non-Compliant (NC)
- Somewhat Compliant (SC)
- Partially Compliant (PC)
- Mostly Compliant (MC)
- Fully Compliant (FC)

The compliance scale maturity levels formalize and validate the maturity of the organization's HIPAA compliance program. Finally, the HITRUST CSF defines maturity ratings to help an organization understand how effectively they are addressing their compliance and security requirements. The defined HITRUST maturity ratings range from Level 1 (lowest) to Level 5 (highest).

Closing Remarks for Senior Executives

Don't wait until it's too late. Tomorrow starts now! Establish a credible HIPAA compliance program aligned with the HITRUST CSF. Prioritize the completion of HITRUST certification. Applying the HITRUST CSF to address HIPAA mandates requires the following key steps:

1. Integrate the HITRUST Risk Management Framework into your information protection program.
2. Conduct a comprehensive HITRUST CSF Self-Assessment.
3. Perform HITRUST CSF Validation and Certification.
4. Manage and maintain HITRUST CSF Certification– ***Continually***

The bottom-line recommendation for HIPAA compliance:

HITRUST CSF = *Credible* **HIPAA Compliance!**

The HITRUST CSF certification helps support an organization's assertion of HIPAA compliance. When you think of HIPAA compliance, think HITRUST CSF certification. Get started now!

Reference

https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html?language=en

ecfirst

HITRUST CSF Strategy Workshop

1-Day Cyber Security & Compliance Brief

Learning Objectives

In this one-day strategy workshop focused on security and compliance, you will:

- Examine business compliance priority based on 2018 regulatory enforcement
- Learn how to align cyber and compliance priorities with the HITRUST CSF framework
- Leverage the HITRUST CSF standard to establish a credible cybersecurity program
- Walk thru HITRUST CSF fundamentals
- Identify next steps to launch initiatives to achieve HITRUST CSF certification

Target Audience

Private On-Site Workshop

Review select HITRUST CSF policies, live, in-class!

John Schelewitz | John.Schelewitz@ecfirst.com | +1.480.663.3225

Delivering Everything Compliance. Everything Security.

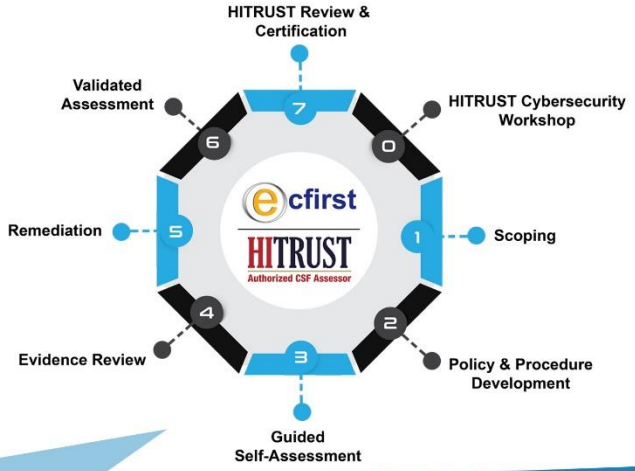
1000s of Clients | Clients in all 50 States | Clients on 5 Continents

HITRUST Authorized CSF Assessor

Professional Services

As a HITRUST Authorized CSF Assessor, ecfirst delivers comprehensive services to assist your organization with pre-assessment, self-assessment, validation and certification. Areas ecfirst can collaborate with your organization, include:

- Perform a guided HITRUST CSF self-assessment
- Partner with your organization to complete HITRUST CSF validation and certification
- Customized development of HITRUST CSF policies
- Creation of tailored HITRUST CSF procedures
- Delivery of HITRUST CSF Strategy Workshop
- Access to in-depth training and certification programs including CHP, CSCS™, CCSA℠



BRG
Berkeley Research Group

"I just wanted to take a moment and say thank you. Thank you and the excellent team at ecfirst for hard work, late hours and diligence during the first round of our HITRUST certification, and now working on our annual risk management and HIPAA compliance assessment."

"We at BRG are always looking to improve and enhance our compliance and cybersecurity posture. This is an area of executive and strategic priority for our organization to secure confidential client information. From HIPAA compliance, cybersecurity pen tests, to the HITRUST certification engagement, we have found ecfirst to be an exceptional partner that labored incredibly hard for us, with us. The ecfirst insight and diligence to ensuring HITRUST certification mandates are met led to us completing our engagement on budget and time. We look forward to deeper collaboration with ecfirst in the cybersecurity space in the future. I know you are personally committed and engaged to ensure BRG success with each engagement. I continue to recommend ecfirst highly and often!"

Chip Goodman | Vice President of Information Technology

BrightOutcome
COLLABORATIVE SYMPTOM MANAGEMENT

"BrightOutcome is focused in improving patient health outcomes across the continuum of care. BrightOutcome is deeply committed to securing patient information across our systems and Web-based applications. We have been working with Ali Pabrai and his wonderful team at ecfirst since 2012."

"The ecfirst team literally helped us build our HIPAA practices from ground up, allowing us to offer secure HIPAA-compliant eHealth and health IT solutions to our customers across the U.S. We are actively taking the logical next step in working with ecfirst to pursue the HITRUST certification in order to further expand our market. We see the partnership with ecfirst as an integral part of our business strategy and have been extremely satisfied with the quality and value of the services that ecfirst has rendered."

DerShung Yang | Founder & President

John Schelewitz | John.Schelewitz@ecfirst.com | +1.480.663.3225

Delivering Everything Compliance. Everything Security.

1000s of Clients | Clients in all 50 States | Clients on 5 Continents

HITRUST Authorized CSF Assessor

FEATURED SPEAKER WORLDWIDE

Uday Ali Pabrai

Cybersecurity & Compliance Expert

ISACA 2017 TOP-RATED SPEAKER ★★★★★

Ali Pabrai, MSEE, CISSP (ISSAP, ISSMP), HITRUST (CCSFP), Security+, a cybersecurity & compliance expert, is the chairman & chief executive of ecfirst.

A highly sought after professional, he has successfully delivered solutions to U.S. government agencies, IT firms, healthcare systems, legal & other organizations worldwide.

Mr. Pabrai has led numerous engagements worldwide for ISO 27001, PCI DSS, NIST, GDPR, HITRUST CSF and HIPAA/HITECH. Mr. Pabrai served as an Interim CISO for a health system with 40+ locations in USA. ecfirst is an approved HITRUST CSF Assessor.

Mr. Pabrai has presented passionate briefs to tens of thousands globally, including the USA, United Kingdom, France, Taiwan, Singapore, Canada, India, UAE, Saudi Arabia, Philippines, Japan, Ireland, Canada, Saudi Arabia, Bahrain, Jordan, Egypt, Ghana and other countries. Conferences Mr. Pabrai has been featured at include AHIMA, HCAA, ISACA CSX, HIMSS, InfraGard (FBI), ISSA, HIPAA Summit, Google Privacy & Security Summit, Microsoft Tech Summit, Internet World, DCI Expo and hundreds of others.

He is a globally renowned speaker who has been featured as a keynote as well as moderated cybersecurity conferences. Mr. Pabrai is the author of several published works. Clients that Mr. Pabrai has delivered to have included the Defense Intelligence Agency (DIA), and the Naval Surface Warfare Center. His career was launched with Fermilab, a U.S. Department of Energy nuclear research entity.

Mr. Ali Pabrai was appointed and served (2017) as a member of the select HITRUST CSF Assessor Council. Mr. Pabrai is a proud member of the InfraGard (FBI).

Mr.Pabrai can be reached at Pabrai@ecfirst.com or +1.949.528.5224.
Control your excitement!

Pabrai @ Global Events

Ascendant Compliance Management · ISSA · himss transforming health through IT · Health Care Compliance Association · Google · Microsoft · CSX Cybersecurity Nexus · AHIMA American Health Information Management Association · HIPAA Summit · wedi · ISACA · AHIP · ASIS International · InfraGard

"We have had the true pleasure of working with Ali Pabrai at conferences all over the world during the past few years – with one unanimous word that keeps resounding among audiences and staff alike – *AWESOME!*

He is a *tremendously engaging and knowledgeable presenter* who is able to *distill the essence of complex cybersecurity topics into comprehensible and actionable components* for both highly skilled, technical audiences as well as those who are just entering or transitioning into the security part of the IT industry.

His "behind the curtain" professionalism and *enthusiastic willingness to help develop, customize and deliver great content paired with his absolute commitment to professionalism as a presenter and "doing what it takes" is a rare combination.*

We greatly look forward to working with Mr. Pabrai each and every time and know he will deliver excellence."

Michael Mach *CMP, CMM, CED*
Conference Program Manager
ISACA

"I have 20+ years of experience in the Healthcare IT industry in a variety of roles including Cybersecurity software and services. During this time I have seen numerous speakers on the topic of Cybersecurity and *Ali Pabrai is among the best.* He covers the state of the industry, healthcare-specific regulations, process, product, best practices and call-to-action takeaways in a manner that can be understood at multiple levels including technical, clinical, supply chain and executive.

Ali also weaves in stories and humor to keep the audience engaged on what can be a dry yet frightening topic. *I highly recommend Ali Pabrai as a speaker, trainer and consultant in this area.*"

Chris Liburdi
Director – Business Development/Business Technology
Vizient

"The professionalism and complete subject matter knowledge make ecfirst the consultants of choice for HIPAA and HITECH information and issues. Our experience with ecfirst was unwavering in addressing all issues and enabling a foundation for an active and vibrant compliance program. Pabrai's leadership was exceptional, very devoted to ensuring all areas were appropriately addressed."

Blake Anderson
Department of Health
State of Utah

Delivering Everything Compliance. Everything Security.

1000s of Clients | Clients in all 50 States | Clients on 5 Continents

HITRUST Authorized CSF Assessor

Published Author

Getting Started with HIPAA — First published book on HIPAA!

UNIX Internetworking — First book on UNIX & Networks!

Internet & TCP/IP Network Security — First book on TCP/IP security!