HITRUST®

HITRUST and HIPAA Safe Harbor

How the HITRUST Approach Meets the Requirements of Having Recognized Security Practices in Place

February 2021

Introduction

On January 5, 2021, the President of the United States signed the HIPAA Safe Harbor Bill, H.R. 7898, into law--amending the existing Health Information Technology for Economic and Clinical Health (HITECH) Act. For healthcare covered entities (CE) and business associates (BA), the key take-way is that it "…require(s) the Secretary of Health and Human Services to consider certain recognized security practices of covered entities and business associates when making certain determinations, and for other purposes." It states that if CEs and BAs can adequately demonstrate that such recognized security practices have been in place for no less than the previous 12 months, the result could be not having to incur additional burden of proof for compliance and avoiding heightened scrutiny from regulators (that typically result in fines).

Read the full bill on the U.S. Government Information website: https://www.govinfo.gov/content/pkg/BILLS-116hr7898enr/pdf/BILLS-116hr7898enr.pdf.

Interpreting "Recognized Security Practices"

The "recognized security practices" that H.R. 7898 states may be determined for use by a CE or BA specifically includes "the standards, guidelines, best practices, methodologies, procedures, and process developed under § 2(c)(15) of the National Institute of Standards and Technology [NIST] Act."[1] The Act authorizes NIST to, "on an ongoing basis, facilitate and support the development of a voluntary, consensus-based, industry-led set of standards, guidelines, best practices, methodologies, procedures, and processes to cost-effectively reduce cyber risks to critical infrastructure (as defined under subsection (e) [of the Act],"[2] of which the Healthcare and Public Health (HPH) Sector is a part. In addition to defining critical infrastructure, Subsection 2(e) also instructs the NIST Director to "incorporate voluntary consensus standards and industry best practices"[3] when developing these standards, guidelines, best practices, methodologies, procedures, and processes.

NIST's response to § 2(c)(15) of the NIST Act was the development and promulgation of the NIST *Framework for Improving Critical Infrastructure Cybersecurity*,[4] commonly referred to as the "NIST Cybersecurity Framework," which "focuses on using business drivers to guide cybersecurity activities and considering cybersecurity risks as part of the organization's risk management processes… [and] provides a common organizing structure for multiple approaches to cybersecurity by assembling standards, guidelines, and practices that are working effectively today."[5] And nowhere is this more clearly expressed than by the Informative References used to help organizations identify "standards, guidelines, and practices common among critical infrastructure sectors that illustrates (sic) a method to achieve the outcomes associated with each [Framework Core] Subcategory."[6]

Informative References in version 1.1 of the NIST Cybersecurity Framework document include CIS CSC, COBIT, ISA 62443-2-1 and 62443-3-3, ISO/IEC 2001, and NIST SP 800-53. Additional Informative References are available from the NIST Online Informative Reference (OLIR) Catalog,[7] "which provides information about the Informative References submitted to and accepted by NIST"[8]

---

[1] An Act to amend the Health Information Technology for Economic and Clinical Health Act to require the Secretary of Health and Human Services to consider certain recognized security practices of covered entities and business associates when making certain determinations, and for other purposes, H.R. 7898, 116th Congress (2019-2020). Available from https://www.congress.gov/bill/116th-congress/house-bill/7898/text?r=2&s=1.

[2] National Institute of Standards and Technology Act, 15 USC §§ 271 – 286. Available from https://uscode.house.gov/view.xhtml?path=/prelim@title15/chapter7&edition=prelim.

[3] Ibid.

[4] NIST (2018, 16 Apr). Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1. Gaithersburg, MD: Author. Available from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

[5] Ibid., p. v.

[6] Ibid., p. 46.

[7] NIST (2020a). Projects: OLIR: National Online Informative References Program: Informative References Catalog. Available from https://csrc.nist.gov/projects/olir/informative-reference-catalog.

[8] NIST (2020b). Glossary: OLIR Catalog. Available from https://csrc.nist.gov/glossary/term/OLIR_Catalog.

and "contains all the Reference Data—Informative References and Derived Relationship Mappings (DRMs)—for the National Online Informative References (OLIR) Program.[9] All Reference Data in the Informative Reference Catalog has been validated against the requirements of NIST Interagency Report (IR) 8278A, National Online Informative References (OLIR) Program: Submission Guidance for OLIR Developers."[10,11] The NIST OLIR Catalogue contains Informative References such as NISTIR 8286, NIST SP 800-171, NIST SP 800-181, and the HITRUST CSF®.

However, while organizations are essentially free to select such practices (controls) as they deem necessary to achieve these cybersecurity outcomes, the Health Insurance Portability and Accountability Act (HIPAA) Security Rule[12] requires CEs and BAs to "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic Protected Health Information [ePHI],[13]"… implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level,[14]… [and] protect against any reasonably anticipated threats or hazards to the security and integrity of such information."[15] The risk assessment (synonymous with risk analysis)[16] plays an essential role in designing controls or selecting controls from one or more Informative References that would ultimately address the outcomes specified by the NIST Cybersecurity Framework Core Subcategories.

Unfortunately, many if not most of the Informative References currently available (either in the Framework document or the OLIR Catalog) do not provide a mechanism to select an appropriate set of controls to adequately protect ePHI, i.e., they do not incorporate a risk analysis-based approach to comprehensive control selection nor provide additional tailoring guidance for the controls they do provide. Notable exceptions include ISO 27001, which provides additional guidance for healthcare organizations but no specific tailoring guidance; NIST SP 800-53, which provides three minimum security baselines selectable by completing the risk analysis used to generate the baselines and additional tailoring guidance for those baselines; and the HITRUST CSF, which leverages the risk analysis performed by NIST as an industry-level overlay of the NIST SP 800-53 moderate impact minimum security baseline, tailored in accordance with NIST guidance.[17]

However, while similar to other NIST SP 800-53 control overlays like those produced by the Centers for Medicaid and Medicare (CMS),[18,19] the HITRUST CSF is significantly more comprehensive in that it integrates and harmonizes multiple regulatory requirements and best practice frameworks relevant to industry while allowing its requirements to be dynamically tailored to different types and sizes

9 Keller, N., Quinn, S., Smith, M., Scarfone, K., and Johnson, V. (2020, Nov). National Online Informative References Program: Program Overview and OLIR Uses (NISTIR 8278). Gaithersburg, MD: NIST. Available from https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8278.pdf.

10 Barrett, M., Smith, M., Keller, N., and Scarfone, K. (2020, Nov). National Online Informative References (OLIR) Program: Submission Guidance for OLIR Developers (NISTIR 8278A). Gaithersburg, MD: NIST. Available from https://nvlpubs.nist.gov/nistpubs/ir/2020/ NIST.IR.8278A.pdf.

11 NIST (2020a).

12 U.S. Dept. of Health and Human Services, HHS (2013, 16 Mar). HIPAA Administrative Simplification: Regulation Text (45 CFR Parts 160, 162, and 164), § 164. Available from https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf.

13 HHS (2013, 16 Mar), § 164.308(a)(1)(ii)(A).

14 HHS (2013, 16 Mar), § 164.308(a)(1)(ii)(B).

15 HHS (2013, 16 Mar), § 164.306(a)(1).

16 NIST (2020c). Glossary: Risk Assessment. Available from https://csrc.nist.gov/glossary/term/risk_assessment.

17 Cline, B. (2017, Sep). Leveraging a Control-Based Framework to Simplify the Risk Analysis Process, ISSA Journal, 15(9), pp. 39 – 42. Available from https://hitrustalliance.net/content/uploads/Leveraging-a-Control-Based-Framework-to-Simplify-the-Risk-Analysis-Process.pdf.

18 CMS (2017, 21 Nov). CMS Acceptable Risk Safeguards, version 3.1 (CMS ARS). Available from https://www.cms.gov/Regulations-and-Guidance/Guidance/Manuals/Downloads/ 117_Systems_Security_MAC_ARS.pdf.

19 CMS (2015, 10 Nov). MARS-E document Suite, Volume II: Minimum Acceptable Risk Standards for Exchanges (MARS-E), Version 2.0. Washington, D.C.: Author. Available from https://www.cms.gov/CCIIO/Resources/Regulations-and-Guidance/Downloads/2-MARS-E-v2-0-Minimum-Acceptable-Risk-Standards-for-Exchanges-11102015.pdf.

of organizations based on relevant organizational, technical, and regulatory risk factors. In fact, the risk analysis approach HITRUST® uses to produce the HITRUST CSF forms the basis for HPH Sector guidance on how to implement the NIST Cybersecurity Framework.

Produced in 2016 under the auspices of the Critical Infrastructure Partnership Advisory Council (CIPAC), a private-public partnership created "to facilitate interaction between governmental entities and representatives from the community of critical infrastructure owners and operators,"[20] the *Healthcare Sector Cybersecurity Framework Implementation Guide*, version 1.1 addresses the concept of control framework-based risk analysis as a viable approach to control specification and features the HITRUST CSF as a healthcare-specific implementation of the approach.[21] The second version of the guide is currently in draft, expands on the use of control framework-based risk analysis and tailoring to include similarly comprehensive Informative References, and is expected to be released in early 2021.

And finally, the use of programs and services like those provided by the HITRUST Approach™ to help CEs and BAs address HIPAA compliance is not without precedent. In 2014, an Office of Civil Rights (OCR) spokesperson stated:

> ***"While OCR does not endorse any particular credentialing or accreditation program, we certainly encourage covered entities and business associates to build strong compliance programs internally. Many of these credentialing/accreditation programs can help them do so…. OCR considers mitigation and aggravating factors when determining the amount of a civil monetary penalty, and these include the entity's history of prior compliance. An entity with a strong compliance program in place, with the help of a credentialing/accreditation program or on its own, would have that taken into account when determining past compliance."*** [22]

A 2018 Government Accountability Office (GAO) report on NIST Cybersecurity Framework implementation also stated HPH sector officials encourage alignment with existing cyber guidelines and specifically cited the HITRUST CSF as an example of how an organization can demonstrate 'compliance' with the NIST Cybersecurity Framework.[23]

H.R. 7898 simply *obligates* OCR to provide safe harbor to CEs and BAs that appropriately implement approaches like HITRUST that meet the new legislative requirements.

It is also worth noting that HITRUST introduced the new Regulatory Assistance Center in December 2020 to aid organizations that have a HITRUST CSF Certification and are preparing for or undergoing a regulatory audit. This no-cost assistance includes guidance on how HITRUST CSF Assessment Reports can and should be leveraged to demonstrate compliance, including how specific requirements are met or how best to respond relating to a specific inquiry. The Center is staffed with security and privacy professionals, attorneys, and other experts familiar with the HITRUST CSF, HITRUST Assurance Program, and HIPAA regulations.

---

20 Cybersecurity & Infrastructure Security Agency, CISA (2020a). About CISA: Critical Infrastructure Partnership Advisory Council. Available from https://www.cisa.gov/critical-infrastructure-partnership-advisory-council.

21 Joint HPH Sector Cybersecurity Working Group (2016, May). Healthcare Sector Cybersecurity Framework Implementation Guide, version 1.1. Washington, D.C.: CIPAC. Available from https://us-cert.cisa.gov/resources/cybersecurity-framework.

22 McGee, M. (2014, 30 Apr). How Texas is Boosting HIPAA Compliance: New Certification Program Builds on HITRUST Effort, Gov Info Security. Available from https://www.govinfosecurity.com/how-texas-boosting-hipaa-compliance-a-6800.

23 GAO (2018, Feb). Report to Congressional Committees on Critical Infrastructure Protection: Additional Actions are Essential for Addressing Cybersecurity Framework Adoption (GAO-18-211), Gaithersburg, MD: Author, p. 15. Available from https://www.gao.gov/assets/700/690112.pdf.

Conclusion

While H.R. 7898 does not specifically name HITRUST as a "recognized security practice," the HITRUST Approach incorporates recognized security practices and provides a comprehensive methodology to demonstrate appropriate adoption and evidence of compliance. It's clear the federal government recognizes the HITRUST Approach to risk management and implementation of the NIST Cybersecurity Framework by HPH Sector organizations, including HIPAA CEs and BAs. Furthermore, the anticipated Government Coordinating Council (GCC) and Sector Coordinating Council's (SCC) joint release of the next version of the HPH Sector Cybersecurity Framework Implementation Guide by HHS will further establish the HITRUST CSF and CSF Assurance Program—the two primary components of the HITRUST Approach—as a "recognized security practice."

Leveraging HITRUST to demonstrate compliance with HIPAA has numerous advantages in terms of efficiency and effectiveness. The HITRUST Approach, when fully implemented and evidenced with a HITRUST CSF Certification, ensures covered entities and business associates can meet compliance requirements of the HIPAA Security and Breach Rule.

As a leading standards and certification organization, HITRUST has advocated and encouraged establishing safe harbor for many years under the belief that it will support organizations who are doing the right thing, incentivize increased investment in cybersecurity, and improve patient safety.

Resources

- **HITRUST Approach to HIPAA Compliance** – Download this free guide, which documents HITRUST controls as they relate to HIPAA's Security and Breach Notification Rules. The guide includes instructions, a support and responsibilities table, and a HIPAA compliance checklist that can be leveraged as organizations pursue their HIPAA compliance objectives. Click here to download the guide.
- **HITRUST Regulatory Assistance Center** – The new HITRUST Regulatory Assistance Center was created to aid organizations that have a HITRUST CSF Certification and are preparing for or undergoing a regulatory audit. This no-cost assistance includes guidance on how HITRUST CSF Assessment Reports can and should be leveraged to demonstrate compliance, including how specific requirements are met or how best to respond relating to a specific inquiry. The Center is staffed with security and privacy professionals, attorneys, and other experts familiar with the HITRUST CSF, HITRUST Assurance Program, and HIPAA regulations. Click here to learn more about the HITRUST Regulatory Assistance Center.
- **HITRUST Compliance and Reporting Pack for HIPAA** – The MyCSF information risk SaaS platform significantly streamlines how organizations capture and present HIPAA compliance evidence. Within MyCSF, the information is automatically consolidated into a compliance report formatted by HIPAA control and populated with evidence and documentation that can be shared directly with investigators. The HITRUST Compliance and Reporting Pack for HIPAA will be available to all HITRUST MyCSF subscribers, effective March 2021. Learn more.

About HITRUST

HITRUST's comprehensive approach to risk management and enhanced support options are largely why more than 80 percent of U.S. hospitals, 85 percent of U.S. health insurers, and many other covered entities and business associates continue to leverage the HITRUST Approach to aid their HIPAA compliance initiatives.

Since it was founded in 2007, HITRUST has championed programs that safeguard sensitive information and manage information risk for organizations across all industries and throughout the third-party supply chain. In collaboration with privacy, information security, and risk management leaders from the public and private sectors, HITRUST develops, maintains, and provides broad access to its widely adopted common risk and compliance management frameworks as well as related assessment and assurance methodologies.

To learn more, please email info@hitrustalliance.net or visit https://hitrustalliance.net/hitrust-for-hipaa/.

HITRUST®

855.HITRUST
(855.448.7878)
www.HITRUSTAlliance.net