HITRUST®

HITRUST and HIPAA

How the HITRUST Approach Can Help Healthcare Organizations Demonstrate Compliance with HIPAA

HITRUST CSF®

HITRUST Assessment Portfolio

HITRUST Assurance Program

HITRUST Assessment XChange™

Regulatory Assistance Center

MyCSF® Compliance Pack for HIPAA

HITRUST Threat Catalogue®

April 2023

Table of Contents

Introduction

From its inception, HITRUST[1] has helped healthcare organizations comply with the HIPAA[2] Security Rule through application of its control framework-based approach to risk analysis and control specification[3] as well as support their assertions of compliance through HITRUST Assessment and Certification.[4] And now HITRUST provides even more products and services[5] that support all sizes and types of organizations with various levels of risk to help them understand their HIPAA compliance obligations, provide appropriate assurances to regulators and business partners, and achieve safe harbor pursuant to the HITECH Act as amended on 5 Jan 2021 by H.R. 7898—the [HIPAA] Safe Harbor bill.[6]

To best understand how HITRUST can help, we address two separate but related aspects of HIPAA compliance and safe harbor: (1) implementing a HIPAA-compliant information protection program that meets safe harbor requirements, and (2) providing meaningful assurances to relying parties about the HIPAA-compliant information protection program.

Implementing the Information Protection Program

Addressing HIPAA Requirements

The HIPAA Security Rule enumerates specific Standards and Implementation Specifications, some of which are 'required' in the sense they must generally be implemented as stated and others which are 'addressable' in the sense they are not optional but rather have additional flexibility in how they are implemented if it's considered reasonable and appropriate to do so.[7] However, simply doing 'something' for each of the Standards and Implementation Specifications in the Rule does not—and arguably cannot—guarantee compliance.

In fact, any approach that relies on a static set of safeguards—whether a 'minimum' set of good hygiene practices or even a comprehensive set of leading practices—would likely not satisfy one's obligations under HIPAA. This point was made clear by Linda Sanches of OCR at a 2012 conference presentation when asked if implementing and assessing against requirements outlined in the OCR Audit Protocol[8] would satisfy HIPAA requirements for a risk analysis.[9] Her response was that simply 'complying' with the Protocol would not ensure reasonably anticipated threats to an organization's ePHI have been identified nor that such an arguably limited set of safeguards would ensure its adequate protection. In other words, "No."

In addition to implementing such safeguards, HIPAA Safe Harbor requirements add another compliance criterion to the mix by requiring organizations to demonstrate 'recognized security practices' have been in place for no less than the previous 12 months of any consideration for safe harbor. These "recognized security practices [include] the standards, guidelines, best practices, methodologies, procedures, and process developed under § 2(c)(15) of [NIST] Act,"[10] the most well-known of which is the NIST Cybersecurity Framework.[11] One of the most salient features of the NIST Cybersecurity Framework is the concept of 'informative references',[12] which are intended to help organizations identify "standards, guidelines, and practices common among critical infrastructure sectors" that can help them achieve specific cybersecurity outcomes.

---

1 HITRUST (2021a). HITRUST: Company: About HITRUST. Available from https://hitrustalliance.net/about-us/.

2 Office of Civil Rights, OCR (2013, Mar). HIPAA Administrative Simplification: Regulation Text: 45 CFR Parts 160, 162, and 164 (Unofficial Version, as amended through March 26, 2013). Available from https://www.hhs.gov/sites/default/files/hipaa-simplification-201303.pdf.

3 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.

4 Cline, B. and Vander Wal, K. (2018). The HITRUST CSF and CSF Assurance. Available from https://hitrustalliance.net/uploads/HITRUST-CSF-and-CSF-Assurance.pdf

5 HITRUST (2021b). HITRUST Approach. Available from https://hitrustalliance.net/the-hitrust-approach/.

6 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.

7 Department of Health and Human Services, HHS (2021). What is the difference between addressable and required implementation specifications in the Security Rule? Available from https://www.hhs.gov/hipaa/for-professionals/faq/2020/what-is-the-difference-between-addressable-and-required-implementation-specifications/index.html.

8 HHS (2021). HIPAA Compliance and Enforcement: HIPAA Privacy, Security, and Breach Notification Audit Program: Audit Protocol. Available from https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/ protocol/index.html.

9 Sanches, Linda. 2012. "2012 HIPAA Privacy and Security Audits,"2012 NIST-OCR HIPAA Security Conference – http://csrc.nist.gov/news_events/hiipaa_june2012/day2/day2-2_lsanches_ocr-audit.pdf.

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

11 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.

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

The Healthcare and Public Health (HPH) sector guide on implementation of the NIST Cybersecurity Framework[13]—version 2 of which is currently undergoing review by the U.S. Department of Health and Human Services (HHS)[14] as joint public-private sector guidance—specifically addresses how an appropriate set of safeguards from one or more informative references such as the HITRUST CSF can be used to implement the framework. The HITRUST CSF is relatively unique amongst currently available information references in that it leverages the risk analysis performed by NIST as an industry-level security control overlay[15] of the NIST Special Publication (SP) 800-53[16] moderate impact minimum security baseline, tailored in accordance with NIST guidance[17]—a process HITRUST refers to as control framework-based risk analysis.

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. The HITRUST framework 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 of organizations based on relevant organizational, technical, and compliance risk factors.[20] Organizations can then tailor these 'semi-custom' control specifications to address unique aspects of their threat and operating environments that differentiate them from other organizations with similar risk factors.

To ensure one's ability to demonstrate compliance with the HIPAA Security Rule's risk analysis requirement, HITRUST strongly recommends organizations document the control framework-based risk analysis process(es) used to determine the relevant HITRUST CSF control specification(s)—as well as the rationale and management approval for all its tailoring decisions—even after HHS approves the HPH Sector Cybersecurity Framework Implementation Guide v2 for release.

Specifying Controls

Large Enterprises

Control specification for a large organization is relatively straightforward. The first step is to partition the organization's environment by grouping together information systems, infrastructure, and business units with similar information security requirements so that a common set of organizational, technical, and compliance risk factors can be applied to the HITRUST CSF framework as mentioned earlier.[21] Whether performed manually or within MyCSF[22] by creating a comprehensive r2 Assessment (previously known as a HITRUST CSF Validated Assessment),[23] application of these factors will yield a semi-custom set of control requirements that represent an industry acceptable minimal level of due care needed to manage risk appropriately.[24] HITRUST also provides a Threat Catalogue[25] with a comprehensive list of threats mapped to HITRUST CSF controls, which can help organizations understand how they are controlling relevant threats and subsequently conduct the targeted risk analyses needed to complete the tailoring process as previously mentioned.

Medium and Small Enterprises

There is no single definition of a small to medium-sized enterprise (SME), and the definition can even vary from one industry to another for small organizations in the U.S., but a rough rule of thumb is that a medium-sized business has less than 250 employees while small business

---

[13] 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.

[14] HHS (2021). About HHS. Available from https://www.hhs.gov/about/index.html.

[15] NIST (2021). Glossary: Security Control Overlay. Available from https://csrc.nist.gov/glossary/term/ security_control_overlay.

[16] Joint Task Force Initiative, JTFI (2013, Apr). Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53, revision 4). Gaithersburg, MD: NIST. Available from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

[17] Ibid., pp. 30-32.

[18] Centers for Medicaid and Medicare, 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.

[20] Cline, B. and Vander Wal, K. (2018).

[21] Sheth, B. (2019, Mar). CSF Assessment Methodology. Available from https://hitrustalliance.net/content/ uploads/CSFAssessmentMethodology.pdf.

[22] HITRUST (2021c). Solutions: MyCSF: Introducing the Next Generation of MyCSF. Available from https://hitrustalliance.net/product-tool/mycsf/.

[23] HITRUST (2021d). Higher Quality and Reliability at Every Level of Assurance. Available from https://hitrustalliance.net/expanded-hitrust-assessment-portfolio/.

[24] Cline, B. (2018, Apr). Understanding HITRUST's Approach to Risk vs. Compliance-based Information Protection: Why framework-based risk analysis is crucial to HIPAA compliance and an effective information protection program, pp. 12, 15. Available from https://hitrustalliance.net/documents/csf_rmf_related/ RiskVsComplianceWhitepaper.pdf.

[25] HITRUST (2021e). HITRUST Threat Catalogue. Available by completing the licensing agreement available from https://hitrustalliance.net/hitrust-threat-catalogue-license-agreement/.

generally has less than 50.[26] SMEs make up the majority of businesses in the world and are responsible for many new products and services due to their flexibility and innovation. However, the U.S. government also recognizes that smaller organizations do not have the same capabilities and resources as their larger counterparts and "bear a disproportionate share of regulatory costs and burdens."[27]

U.S. federal agencies are subsequently required to develop more accessible sources of information on regulatory and reporting requirements for small entities and create a regulatory environment that is more cooperative and less punitive in nature.[28] In addition, the HIPAA Security Rule specifically allows for a certain 'flexibility of approach' in selecting the security measures needed to "reasonably and appropriately implement the [Rule's] Standards and Implementation Specifications,"[29] which small organizations may also leverage. Allowable factors include the *organization's size* [emphasis added], complexity, and capabilities; technical infrastructure, hardware, and software capabilities; cost of required security measures; and the likelihood and severity of the potential risks being controlled.

HITRUST takes a similar approach by further tailoring HITRUST CSF control requirements to help address the needs of these types of organizations.

Medium-Size Enterprises

Once its environment is partitioned as previously discussed for large organizations, a medium-size organization has two options for specifying an appropriate set of HITRUST CSF control requirements. The first is to take the same approach as a large organization in applying risk factors to the HITRUST CSF. The organization would then use the HITRUST Threat Catalogue to help identify threats that are being over controlled and further tailor CSF control requirements based on NIST guidance and the factors allowed under HIPAA's flexibility of approach mentioned earlier. Alternatively, a medium-size organization could select the new HITRUST i1[30] requirements as an initial baseline control specification. The HITRUST i1—or "Implemented, 1-Year" (i1) Validated Assessment—is intended to provide an appropriate level of assurance for organizations that present a moderate-level of risk by specifying industry-accepted 'best' or 'leading' practices suitable for these types of entities, including related coverage of the HIPAA Security Rule. Organizations should then perform one or more targeted risk analysis leveraging the HITRUST Threat Catalogue to (1) help identify threats and associated risks that may be under controlled and/or do not sufficiently address the HIPAA Security Rule's Standards and Implementation Specifications and (2) add relevant control requirements from the HITRUST CSF library to address identified 'control gaps' as needed.

Small Enterprises

Like their medium-size counterparts, small organizations also have two options when leveraging the HITRUST CSF for their risk analysis: they can select the requirements used in a HITRUST i1 Assessment and remove requirements to prevent threats from being over controlled. Alternatively, they can select the good security hygiene requirements contained in a HITRUST "Essentials, 1-year" (e1) Assessment—and add requirements from the i1 or r2 to help ensure (1) threats are not being under controlled and that (2) the HIPAA Security Rule's Standards and Implementation Specifications are adequately addressed. However, in no case should a small organization remove control requirements that are contained in the original e1 control specification without performing a valid risk analysis and ensuring management formally accepts the risk of not implementing the good security hygiene practice(s).

Providing Assurances about the Information Protection Program

As the organization implements its HIPAA-compliant information security program, the next step is to provide assurances to internal and external stakeholders such as executive management, boards of directors, business partners, and regulators. These types of assurances are normally provided through some sort of security controls assessment; however, providing assurances to OCR about one's compliance with the HIPAA Security Rule can often be more involved as one must be able to demonstrate, at a minimum:

1. The controls implemented or to be implemented by the organization are based on a valid risk analysis;
2. Risk is actively managed;
3. Controls adequately address the HIPAA Security Rule's Standards and Implementation Specifications; and,
4. For those seeking safe harbor, the controls are based on one or more recognized security practices.

---

[26] CFI (2021). Small and Medium-sized Enterprises (SMEs): Independent businesses with around 50-250 employees.
Available from https://corporatefinanceinstitute.com/resources/knowledge/other/small-and-medium-sized-enterprises-smes/.

[27] The Small Business Regulatory Enforcement Fairness Act of 1996 (SBREFA), Pub. L. No. 104-121, as amended by Pub. L. No. 110-28 (May 25, 2007).
Available from https://www.fws.gov/policy/library/rgpublaw104-121.pdf.

[28] HHS (2021b). Health Information Privacy: How can a small provider implement the standards in [the] Security Rule?
Available from https://www.hhs.gov/hipaa/for-professionals/faq/2007/how-can-a-small-provider-implement-the-standards-in-security-rule/index.html.

[29] OCR (2013, Mar), p. 63.

[30] HITRUST (2021d).

The HIPAA Risk Analysis

To be 'HIPAA-compliant,' organizations must "conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability"[31] (CIA) of the ePHI it holds. This requirement is foundational to the HIPAA Security Rule and, while requirements around risk analysis are common today, was truly ground-breaking at the time of its issuance.

Unfortunately, one of the most often cited deficiencies in the second phase of the OCR HIPAA audit program conducted in 2016 and 2017 was around this requirement.[32] Documentation requested for the audits included current and prior risk analyses and their results, supporting policies and procedures around risk analysis and its implementation, and evidence demonstrating the actual implementation of the risk analysis process, how it is available to responsible stakeholders, and that this documentation is periodically reviewed and updated, as needed. However, the audits indicated that healthcare organizations, in general, fail to:

- "Identify and assess the risks to all of the ePHI in their possession.
- "Develop and implement policies and procedures for conducting a risk analysis.
- "Identify threats and vulnerabilities, to consider their potential likelihoods and impacts, and to rate the risk to ePHI.
- "Review and periodically update a risk analysis in response to changes in the environment and/or operations, security incidents, or occurrence of a significant event.
- "Conduct risk analyses consistent with policies and procedures.

"Failure to document any efforts to develop, maintain and update policies and procedures, and to use them to conduct a risk analysis, was common."[33]

The HITRUST Approach can help healthcare organizations address many of these issues. For example, HITRUST CSF Control Reference 07.a, Inventory of Assets, requires organizations to conduct and formally document a complete inventory of sensitive information assets, including ePHI.[34] The HITRUST quasi-quantitative control implementation maturity model[35] evaluates every control requirement for the existence of a relevant policy statement or similar mandate and procedures that support the requirement's implementation, including the implementation of risk analysis as addressed by 03.b, Performing Risk Assessments.[36]

HITRUST CSF Control Reference 03.b also requires organizations to perform threat and vulnerability analysis consistent with HHS guidance,[37] and the HITRUST Threat Catalogue supports the analysis of excessive residual risk due to control non-compliance by providing a comprehensive list of threats, threat-to-HITRUST CSF control mappings, non-contextual impact ratings for each control, and an estimate of the likelihood a control will fail based on the assessed maturity of selected requirements via one or more HITRUST Assessments. However, while HITRUST supports the performance of a risk analysis, it is the organization's responsibility to conduct and document their risk analysis, which includes everything from the selection of appropriate risk factors for initial tailoring of HITRUST CSF control requirements as well as the additional tailoring needed to ensure adequate protection of its ePHI.

In addition, HITRUST CSF Control Reference 03.b requires they periodically review and revise their risk analyses when significant changes in their operational or threat environment occurs, and the HITRUST CSF control implementation maturity model also helps ensure the organization's policies and procedures are reflective of this approach and that they conduct their analyses accordingly.

HIPAA Risk Management Requirements

HIPAA's security risk management requirement is narrowly focused on the implementation of "security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level"[38] consistent with the risk analysis requirement to ensure the CIA of ePHI and protect it against any

---

[31] OCR (2013, Mar), p. 64.

[32] OCR (2020, Dec). 2016-2017 HIPAA Audits Industry Report. Available from https://www.hhs.gov/sites/default/ files/hipaa-audits-industry-report.pdf.

[33] Ibid., p. 27.

[34] HITRUST (2021, Sep), pp. 235 – 241.

[35] Cline, B., Huval, J., and Sheth, B. (2020, Sep). Evaluating Control Maturity Using the HITRUST Approach: Quasi-quantitative scoring based on the HITRUST CSF security and privacy control implementation maturity model. Available from https://hitrustalliance.net/content/uploads/Evaluating-Control-Maturity-Using-the-HITRUST-Approach.pdf.

[36] HITRUST (2021, Sep), pp. 132-139.

[37] HHS (2010, 14 Jul). Guidance on Risk Analysis Requirements under the HIPAA Security Rule.
Available from https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf.

[38] OCR (2013, Mar), p. 64.

reasonably anticipated threats. In practice, managing risk means gaps between (i) the organization's 'to be' or target state derived from the risk analysis and (ii) its current state as described by one or more control gap assessments (or similar) are being actively addressed.

Documentation requested by OCR during the 2016-2017 audits included evidence demonstrating the organizations efforts to manage risks, supporting policies and procedures around risk management and its implementation, evidence demonstrating that current and ongoing risks are reviewed and updated, how it is available to responsible stakeholders, and that this documentation is periodically reviewed and updated, as needed.[39]

Whether because the risk analysis is an integral part of the risk management process (and is in fact the first step in the HITRUST Approach) or some other reason (such as the scope of the controls an organization is generally required to implement and maintain), OCR's phase II audits similarly indicated the vast majority of organizations that underwent a phase 2 audit failed to manage risk appropriately. Issues included:

- A lack of necessary focus on technical safeguards,
- A misunderstanding of their vulnerabilities and risks and how they should be mitigated,
- Incomplete evidence of risk management,
- A failure to implement remediation plans around encryption in a reasonable timeframe, and
- A failure to update their risk management plans.

HITRUST helps organizations address these issues by providing a comprehensive control library with prescriptive technical controls that are selected based on relevant risk factors. By properly scoping their environment and applying these factors—whether manually or in the HITRUST MyCSF® platform—organizations can generate what NIST refers to as a target profile,[40] which provides a future or 'to be' state (specification) of information security controls and establishes its risk target. By comparing the current profile or 'as is' state established through one or more control assessments (or similar mechanism, such as control status or performance metrics), an organization can identify control gaps that contribute to excessive residual risk due to its failure to fully implement the target profile. Organizations may select a comprehensive HITRUST r2 Assessment for a complete understanding of its current profile or they may choose to assess purposive samples of its specified controls—such as through an e1 Assessment, or the standard i1 of r2 Assessment used for HITRUST Certification—to provide reasonable assurances at a reasonable cost.

Note it is generally up to the relying party to determine the level of assurance required for a particular use case. In the case of HIPAA compliance, a HITRUST Assessment can and does provide evidence that specific HITRUST CSF control requirements that map to the HIPAA Security Rule's Standards and Implementation Specifications have been implemented, how well they have been implemented, and how the organization intends to address identified gaps in implementation. Depending upon specific concerns around a particular audit or investigation, OCR may request additional assessments or other information about the state of an organization's information risk management program, implemented controls, and relevant changes due to changing threat and operational environments.

At no time should an organization simply submit a HITRUST Assessment—even a comprehensive r2 Assessment—to demonstrate compliance with the HIPAA Security Rule. In fact, OCR stated that documentation of security activities of a third-party security vendor without substantiation of its need by a valid risk analysis as a common failure.[41] Additional information such as specific policies and procedures and additional information around specific control requirements (e.g., encryption), associated deficiencies, and their remediation that is not addressed in a standard r2, e1, i1 Assessment may be—and often is—required.

The Rest of the HIPAA Security Rule

HITRUST CSF control requirements that support the HIPAA Security Rule are mapped to relevant Standards and Implementations Specifications, the selection of which is determined by an entity's organizational, technical, and compliance risk factors. Generally, the more risk an organization presents, additional and more robust requirements are specified to help control that additional risk.

The best approach to providing assurances around an organization's compliance with the HIPAA Security Rule is a comprehensive HITRUST r2 Assessment as this will provide evidence around the majority if not all the controls specified from a risk analysis; however, such an assessment can be quite costly, time intensive, and impactful to healthcare operations. For this reason, HITRUST spearheaded the concept of 'reasonable assurance

[39] OCR (2020, Dec), p. 30.

[40] NIST (2018, 16 Apr), p. 4.

[41] OCR (2020, Dec), pp. 27-28.

at a reasonable cost' by offering assessments based on a purposive sample of the control requirements that make up an organization's target profile. We also help organizations understand the 'rely-ability' of a particular approach to providing assurance, i.e., the ability to rely upon the evidence provided by the approach that is subsequently used to assert compliance.[42]

The choice of a e1, i1, and/or standard r2 Assessment option should generally be based on the size/complexity of the organization being assessed and be consistent with the approach used by an organization to complete their risk analysis and specify the control requirements in their target profile. Information on HIPAA-relevant control requirements not included in the chosen assessment will need to be generated separately, e.g., from other internal or external audits or dashboards/reports from automated systems.

However, there may be some instances in which an organization may need or simply want to respond to an OCR audit or investigation with a more limited set of information about their programs, similar to how organizations triage[43] third parties to obtain HIPAA-required 'satisfactory assurances'.[44] Although we can't address every contingency, one example of such a scenario would be a medium-size business associate that may have used a tailored HITRUST i1 to specify control requirements for its information security program but—until an OCR inquiry—only had a business need to provide a HITRUST e1 Assessment to the covered entities it supports. In this case, the organization could potentially provide the results of (1) a tailored i1 along with an explanation of how it was tailored to address the risk analysis requirement and (2) the results of its latest e1Assessment along with additional information around its control gap analysis and remediation plans to address the risk management requirement. The latter would also partially address the remaining HIPAA Standards and Implementation Specifications until it is able to provide an i1Assessment, assuming OCR even asks for it.

Even if an organization uses a HITRUST r2 Assessment that includes HIPAA compliance, there may be a need to provide additional information to OCR upon request. For example, suppose a very specific security incident is reported to OCR but related controls are not part of the purposive sample of control requirements included in the r2. The organization could then use the MyCSF Compliance and Reporting Pack for HIPAA to identify those requirements and help generate the output specific to those requirements.

HIPAA Safe Harbor

Organizations can achieve HIPAA Safe Harbor leveraging the HITRUST Approach[45] by simply following public-private sector guidance on implementation of the NIST Cybersecurity Framework in the healthcare sector.[46] As we mentioned earlier, the guidance addresses how specific informative references like the HITRUST CSF can help organizations address the HIPAA Security Rule's Standards and Implementation Specifications, including those for risk analysis and risk management as well as the objectives or 'outcomes' specified by the NIST Cybersecurity Framework's Core Subcategories.

Evidence supporting an organization's assertions around 'compliance' with the NIST Cybersecurity Framework is provided with every HITRUST r2 Assessment via a NIST Cybersecurity Framework Scorecard,[47] which details how well an organization meets the objective specified by each Core Subcategory based on how well it has implemented relevant HITRUST CSF control requirements. Organizations can also pursue HITRUST's formal certification of the NIST Cybersecurity Framework.

Support by HITRUST Products and Services

We can now highlight/summarize how relevant components of the HITRUST Approach support an organization's attainment of and assurances around its compliance with the HIPAA Security Rule.

---

[42] HITRUST (2020a). How do I know if an Assurance Report is Rely-Able?
Available from https://hitrustalliance.net/content/uploads/How-Do-You-Know-if-a-CSF-Assurance-Report-is-Rely-able.pdf.

[43] Cline, B. (2019, Oct). HITRUST Third-Party Risk Management (TPRM) Methodology: The Qualification Process: A streamlined approach to qualifying a third party for a business relationship leveraging the HITRUST CSF and Assurance Program. Available from https://hitrustalliance.net/uploads/TPRM-Methodology.pdf.

[44] OCR (2013, Mar), p. 65.

[45] Cline, B. (2021, Feb). HITRUST and HIPAA Safe Harbor: How the HITRUST Approach Meets the Requirements of Having Recognized Security Practices in Place, pp. 2-4.
Available from https://hitrustalliance.net/content/uploads/ HITRUST-and-HIPAA-Safe-Harbor.pdf.

[46] Joint HPH Sector Cybersecurity Working Group (2016, May).

[47] HITRUST (2021f). NIST Cybersecurity Framework Scorecard.
Available from https://hitrustalliance.net/ certification/hitrust-certification-of-the-nist-cybersecurity-framework-certification/.

HITRUST CSF[48]

- Comprehensive library of control requirements that can be further tailored by an organization to meet its specific needs.
    - Provides an industry-level overlay of the NIST SP 800-53 moderate impact baseline.
    - Helps address the HIPAA risk analysis requirement and HHS guidance on risk analysis if scoped and tailored properly.
    - Helps generate an organization's NIST Cybersecurity Framework Target Profile, which also serves as its desired risk target.
- Requirements map to dozens of laws, regulations, standards, and best practices frameworks.
    - Supports the ability to report against multiple authoritative sources such as the NIST Cybersecurity Framework with a single set of control requirements.

HITRUST Threat Catalogue[49]

- Helps organizations conduct various risk analyses consistent with HHS guidance.
    - Provides a complete enumeration of 'reasonably anticipated' threats.
    - Maps enumerated threats to HITRUST CSF controls.
- Future iterations of the Catalogue will support more granular threat and risk analyses.

HITRUST Assurance Program[50]

- Supports HIPAA requirements for risk management and program evaluation.
    - Evaluates control requirements in an organization's Target Profile to create a Current Profile.
    - Identifies control gaps and helps document corrective actions (remediation).
- Provides 'satisfactory assurances' about an organization's information protection program through a variety of assessment options with various levels of 'rely-ability': e1, i1, or r2 (including a comprehensive r2)[51].
    - The e1 is focused on essential good security hygiene practices that address the assurance needs of lower-risk organizations. While falling below the level of assurance conveyed by the more rigorous HITRUST i1 and r2 Assessments, the e1 requires less effort to complete and reliably demonstrates that foundational cybersecurity practices are in place. Generally suitable for small organizations or start-ups to differentiate themselves in the marketplace or provide meaningful assurances to merger and acquisition partners, new business units, or recently deployed technology platforms as well as show justification for more favorable cyber insurance premiums. The e1 can also be used for enterprises that are new to HITRUST to get started and as a milestone to show progress towards an i1 or r2.[52]
    - The i1 builds upon the e1 by including leading security practices to help ensure an organization has implemented a strong and broad cybersecurity program that provides broad protection against current and emerging threats, which can help meet an organization's contractual and compliance obligations as well as provide justification for more favorable cyber insurance premiums. The i1 Assessment also includes requirements which directly map to nearly all of the HIPAA Security Rule, omitting only those HIPAA security rule requirements deemed too industry-specific to be included in an industry-agnostic information protection assessment. SMBs can subsequently utilize a HITRUST i1 as the basis for achieving and maintaining compliance with the HIPAA Security Rule and help demonstrate such compliance with a HITRUST i1 Assessment. And, as the i1 provides the foundation for an r2 Assessment, it can provide a steppingstone for those organizations on the path to a HITRUST r2 Assessment. [53]

---

[48] HITRUST (2021, Sep).

[49] HITRUST (2021e).

[50] HITRUST (2021g). HITRUST Assurance Program. Available from https://hitrustalliance.net/hitrust-assurance-program/

[51] HITRUST (2021d).

[52] HITRUST (2023a). HITRUST e1 Essentials, 1-year (e1) Validated Assessment. Available from https://hitrustalliance.net/certification/hitrust-essentials-1-year-e1-validated-assessment/.

[53] HITRUST (2023b). HITRUST i1 Implemented, 1-year (i1) Validated Assessment.
Available from https://hitrustalliance.net/certification/hitrust-implemented-1-year-i1-validated-assessment/.

- The HITRUST r2 Validated Assessment is considered the gold standard for information protection assurances because of the comprehensiveness of control requirements, depth of review, and consistency of oversight. The r2 offers flexible, tailorable, risk-based control selection to meet the most stringent risk and compliance factors. With a proactive Expanded Practices approach to cybersecurity and more requirement statements than an e1 or i1, the r2 Assessment consistently provides the highest level of assurance for organizations with the greatest risk exposure. The r2 is often used:
    - When assurances are needed over specific authoritative sources or international requirements.
    - For organizations processing large amounts of sensitive data and personal information, including PHI.
    - To Assess Once, Report Many™ for enterprises working in multiple industries with complex regulations such as NIST, PCI DSS, HIPAA, and more.
    - During an r2, the MyCSF® Compliance and Reporting Pack for HIPAA automatically compiles HIPAA compliance evidence.
    - When a NIST Scorecard Report is needed to demonstrate compliance with NIST Cybersecurity Framework controls.
    - When an organization's customer has adopted HITRUST as the required assurance mechanism for doing business.
    - To gain a competitive advantage by strengthening business relationships.
    - To show justification for more favorable cyber insurance premiums.[54]

HITRUST Assessment XChange[55]

- Provides organization's an extension of their third-party risk management program.
- Implements the HITRUST TPRM Methodology's qualification process: a risk-based approach to identifying and providing third-party assurance.
- Supports the generation and exchange of satisfactory assurances as required under the HIPAA Security Rule.

HITRUST MyCSF[56]

- Supports automatic generation of an organization's Target Profile leveraging a control framework-based risk analysis, which also serves as its risk target.
- Provides automated support for e1, i1, and r2 (including comprehensive r2) Assessments.
    - Generates Current Profile.
    - Identifies control gaps.
    - Documents corrective actions.
- Hosts the HITRUST MyCSF Compliance and Reporting Pack for HIPAA.

MyCSF Compliance and Reporting Pack for HIPAA[57]

- Addresses the HIPAA Security and Breach Notification Rules.
- Parses applicable HIPAA requirements to a HITRUST Assessment.
- Helps compile and report on HIPAA-relevant evidence/information.

---

[54] HITRUST (2023c). HITRUST Risk-based, 2-Year (r2) Validated Assessment. Available from https://hitrustalliance.net/certification/hitrust-risk-based-2-year-r2-validated-assessment/.

[55] HITRUST (2020b). HITRUST Assessment XChange. Available from https://hitrustax.com.

[56] HITRUST (2021c).

[57] HITRUST (2021h). HIPAA Compliance, Audits, and the MyCSF Compliance and Reporting Pack for HIPAA.
Available from https://hitrustalliance.net/hipaa-compliance-audits-and-the-mycsf-compliance-and-reporting-pack-for-hipaa/.

Regulatory Assistance Center[58]

- Free resource for organizations with a HITRUST Certification.
- Staffed with security and privacy professionals, attorneys, and other experts familiar with.
    - The HITRUST CSF.
    - HITRUST Assurance Program.
    - HIPAA regulations.
- Provides guidance on how HITRUST Assessment results can be leveraged to demonstrate HIPAA compliance.

Support for Other HIPAA Rules

HITRUST also provides support around an organization's compliance with the HIPAA Data Breach Notification Rule[59] and the HIPAA Privacy Rule.[60]

HIPAA Data Breach Notification Rule

HIPAA requirements for "Notification in the Case of Breach of Unsecured Protected Health Information"[61] are addressed by the HITRUST Approach in the same manner as the HIPAA Security Rule and receive the same support from all HITRUST products and services.

HIPAA Privacy Rule

HITRUST is continuing to develop support for an organization's implementation and attestations of compliance with the HIPAA Privacy Rule.

- The HITRUST CSF contains privacy control requirements that map to the HIPAA Privacy Rule's Standards and Implementation Specifications.
- The HITRUST Threat Catalogue does not currently map privacy controls to related threats.
- The HITRUST Assurance Program can support assessments that include privacy requirements that map to the HIPAA Privacy Rule but does not provide a privacy-specific certification.
- The HITRUST Assessment XChange can support the tracking and exchange of any HITRUST Assessment option in the Assurance Portfolio.
- MyCSF has the capability to generate a comprehensive r2 Assessment with privacy control requirements that map to the HIPAA Privacy Rule.
- The MyCSF Compliance and Reporting Pack for HIPAA does not currently address the HIPAA Privacy Rule.
- The Regulatory Assistance Center can support questions around compliance with the HIPAA Privacy Rule's Standards and Implementation Specifications.

---

[58] HITRUST (2020c). Regulatory Assistance Center: Support for Audits and Regulatory Investigations. Available from https://hitrustalliance.net/regulatory-assistance-center/.

[59] OCR (2013, Mar), pp. 71-73.

[60] Ibid., pp. 73-115.

[61] Ibid., p. 71.

HITRUST®

855.HITRUST
(855.448.7878)
www.HITRUSTAlliance.net