HITRUST

HIPAA Insights

Based upon a HITRUST Essentials, 1-year (e1) Validated Assessment

Chinstrap Penguin Corp

As of October 1, 2026

View this assessment in the
HITRUST Report Center

HITRUST

Contents

Transmittal Letter

October 1, 2026

Chinstrap Penguin Corp
123 Main Street
Anytown, Texas 12345

Through HITRUST's "Assess Once, Report Many" capability made possible through the HITRUST CSF, HITRUST has prepared this Health Insurance Portability and Accountability Act ("HIPAA") Insights Report at the request of Chinstrap Penguin Corp ("the Organization"). This Insights Report contains detailed information regarding the coverage and maturity of controls supporting the Organization's compliance with HITRUST CSF requirements mapping to HIPAA for the scope outlined below, based on a HITRUST Essentials, 1-year (e1) assessment using v11.6.0 of the HITRUST CSF. The Organization can leverage this report to share information regarding their HIPAA compliance efforts with internal and external stakeholders.

The full e1 validated assessment report contains detailed information relating to the maturity of information protection controls as defined by the tailoring factors selected by management of the Organization. It includes detailed assessment results, a benchmark report comparing the Organization's results to industry results, and details on corrective action plans (if applicable). Such detailed information can best be leveraged by relying parties who are familiar with and understand the services provided by the Organization. Those interested in obtaining a copy of the full report should contact the Organization directly.

Scope

The e1 assessment that this Insights Report is based upon included the following platform, facilities, and supporting infrastructure of the Organization ("Scope"):

Platform:

- Customer Central (a.k.a. "Portal") residing at Pelican Data Center

Facilities:

- CP Framingham Manufacturing Facility (Office) located in Framingham, MA, United States of America
- CP Headquarters and Manufacturing (Office) located in Las Vegas, NV, United States of America
- Pelican Data Center (Data Center) managed by Pelican Hosting located in Salt Lake City, UT, United States of America

The Organization's Responsibilities and Assertions

Management of the Organization is responsible for the implementation, operation, and monitoring of the control environment for the Scope. Through execution of this responsibility, and completion of a HITRUST Essentials, 1-year (e1) validated assessment, the Organization asserted that management of the Organization:

- Is responsible for the implementation of information protection controls.
- Disclosed all design and operating deficiencies in their information protection controls which they are aware, including those for which they believe the cost of corrective action may exceed the benefits.
- Is not aware of any events or transactions that have occurred or are pending that would have an effect on the Essentials, 1-year (e1) validated assessment that was performed and used as a basis by HITRUST for issuing that report.
- Is not aware of communications from regulatory agencies concerning noncompliance with or deficiencies regarding the information protection controls that are included within the scope of the Essentials, 1-year (e1) validated assessment.

The HIPAA Security Rule requires healthcare organizations to conduct a risk analysis: "an accurate and thorough assessment of the potential risks to the confidentiality, integrity, and availability of electronic protected health information" ... [to] "protect against any reasonably anticipated threats or hazards to the security and integrity of such information." While numerous HITRUST CSF requirements dealing with the Organization's performance of risk analyses are evaluated during HITRUST CSF assessments, HITRUST CSF assessments are not risk assessments. Management of the Organization is responsible for performing and maintaining a risk analysis which adheres to § 164.308(a)(1)(ii)(a) of the HIPAA Security Rule.

Management of the Organization is also solely responsible for ensuring the Organization's compliance with any legal and/or regulatory requirements, including HIPAA.

External Assessor Responsibilities

External Assessors are authorized by HITRUST based upon a thorough vetting process to demonstrate their ability to perform HITRUST CSF Assessments, and individual practitioners are required to maintain appropriate credentials based on their role in HITRUST assessments. In HITRUST validated assessments, the External Assessor is responsible for the following:

- Reviewing and gaining a detailed understanding of the information provided by the Organization.

- Performing sufficient procedures to validate the control maturity scores provided by the Organization.

- Meeting all HITRUST Assessment criteria described within the HITRUST Assessment Handbook.

HITRUST's Responsibilities

HITRUST is responsible for maintenance of the HITRUST CSF and HITRUST Assurance Program against which the Organization completed the accompanying Essentials, 1-year (e1) validated assessment. HITRUST is also responsible for producing the mappings from various authoritative sources, including HIPAA, to the HITRUST CSF. Additional information about HITRUST's "Assess Once, Report Many" approach and on the HITRUST CSF Assurance Program used to support this compliance assessment can be found on the HITRUST website at https://hitrustalliance.net.

Limitations of Assurance

Parties relying on this report should understand the limitations of assurance specified in the Limitations of Assurance section of this report.

Distribution and Use Restriction

This report is provided exclusively for the internal business use of Example Org. Distribution, publication, or disclosure of this report outside of Example Org, in whole or in part, is prohibited. This document contains recipient-specific identifying information and may be monitored for unauthorized distribution.

HITRUST

HITRUST

HIPAA Scorecard

The tables below provide insights on HIPAA compliance for the environment assessed. Each HIPAA standard/implementation specification listed is assigned a compliance score for the implemented control maturity level. The compliance scores are based on the assessment results of the HITRUST CSF requirement(s) as mapped to the HIPAA standard/implementation specification. The measured and managed control maturity levels are not included in this scorecard, as these control maturity levels were not assessed in the underlying HITRUST CSF assessment as a result of the Organization's assessment tailoring. These mappings can be found in Appendix B of this document.

Per § 164.306(b) of the HIPAA Security Rule, healthcare organizations are allowed flexibility in how they choose to meet the requirements of the HIPAA Security Rule so long as the chosen approach reasonably and appropriately implements the applicable standards and implementation specifications. As such, the Organization may have in place additional controls relevant to their HIPAA Security Rule compliance posture which were not evaluated in the underlying HITRUST assessment and therefore not reflected in this report. The HITRUST assessment underlying this HIPAA Insights Report included the HITRUST CSF requirements that HITRUST mapped to HIPAA given their broad applicability to organizations of all sizes and complexities.

To learn about the HITRUST control maturity evaluation and scoring approach, visit https://hitrustalliance.net/content/uploads/Evaluating-Control-Maturity-Using-the-HITRUST-Approach.pdf.

Scorecard Color Legend

FC	Fully Compliant: The control maturity level's scores across all HITRUST CSF requirements included in the Organization's HITRUST assessment mapped to the HIPAA standard/implementation specification averaged 90 - 100%.
Does Not Apply	Does Not Apply: Based on information provided by the Organization (as outlined in the "Scope of the Assessment" and "Organizational characteristics impacting HIPAA coverage" sections of this document), the HIPAA standard/implementation specification does not apply to the scoped aspects of the Organization.

HITRUST

HIPAA Scorecard

HIPAA Security Rule

Reference	Requirement	Implemented Scoring
164.308: Administrative Safeguards		
164.308(a)(1)(i)	Security management process	FC
164.308(a)(1)(ii)(A)	Risk analysis	FC
164.308(a)(1)(ii)(B)	Risk management	FC
164.308(a)(1)(ii)(C)	Sanction policy	FC
164.308(a)(1)(ii)(D)	Information system activity review	FC
164.308(a)(2)	Assigned security responsibility	FC
164.308(a)(3)(i)	Workforce security	FC
164.308(a)(3)(ii)(A)	Authorization and/or supervision	FC
164.308(a)(3)(ii)(B)	Workforce clearance procedure	FC
164.308(a)(3)(ii)(C)	Termination procedures	FC
164.308(a)(4)(i)	Information access management	FC
164.308(a)(4)(ii)(A)	Isolating health care clearinghouse functions	FC
164.308(a)(4)(ii)(B)	Access authorization	FC
164.308(a)(4)(ii)(C)	Access establishment and modification	FC
164.308(a)(5)(i)	Security awareness and training	FC
164.308(a)(5)(ii)(A)	Security reminders	FC
164.308(a)(5)(ii)(B)	Protection from malicious software	FC
164.308(a)(5)(ii)(C)	Log-in monitoring	FC
164.308(a)(5)(ii)(D)	Password management	FC
164.308(a)(6)(i)	Security incident procedures	FC
164.308(a)(6)(ii)	Response and reporting	FC
164.308(a)(7)(i)	Contingency plan	FC
164.308(a)(7)(ii)(A)	Data backup plan	FC
164.308(a)(7)(ii)(B)	Disaster recovery plan	FC

Reference	Requirement	Implemented Scoring
164.308(a)(7)(ii)(C)	Emergency mode operation plan	FC
164.308(a)(7)(ii)(D)	Testing and revision procedures	FC
164.308(a)(7)(ii)(E)	Applications and data criticality analysis	FC
164.308(a)(8)	Evaluation	FC
164.308(b)(1)	Business associate contracts and other arrangements	Does Not Apply
164.308(b)(2)	Business associate contracts and other arrangements	FC
164.308(b)(3)	Written contract or other arrangement	FC

This section has been truncated for this sample report

HITRUST

Assessment Context

About the HITRUST e1 Assessment and Certification

HITRUST e1 assessments address the need for a continuously-relevant cybersecurity assessment focusing on foundational cybersecurity controls and mitigations for the most pressing cybersecurity threats. Organizations successfully achieving an e1 certification can reliably demonstrate they meet a bar of essential cybersecurity hygiene.

This assessment is designed for lower assurance scenarios (such as those needing greater assurances than achieved through information security questionnaires or readiness assessments but less so than those achieved through more robust, higher effort assessments). However, an e1 assessment can also serve as a starting point for enterprises that are in the early stages of implementing their information security controls.

To ensure foundational cybersecurity is in place, e1 assessments focuses on a pre-set selection of HITRUST CSF requirements curated by HITRUST. While not a compliance assessment, the subject matter does overlap with authoritative sources sharing similar goals (such as CISA Cyber Essentials, Health Industry Cybersecurity Practices for Small Healthcare Organizations, NIST SP 800-171's "Basic" requirements, and NIST IR 7621: Small Business Information Security Fundamentals).

HITRUST's analysis of cyber threat intelligence data from leading threat intelligence providers when curating the controls considered during e1 assessments, e1 is an evolving, threat-adaptive assessment. HITRUST continually evaluates this data in relation to the controls included in the e1 to ensure that the e1 continues to address the most critical cyber threats (such as ransomware, phishing, brute force, and abuse of valid accounts).

Assessment Approach

An Authorized HITRUST External Assessor Organization (the "External Assessor") performed validation procedures to measure the control maturity of the HITRUST CSF requirements and corresponding evaluative elements included in this assessment for the scope of the assessment. These validation procedures were designed by the External Assessor based upon the assessment's scope in observance of HITRUST's CSF Assurance Program Requirements and consisted of inquiry with key personnel, inspection of evidence (e.g. access lists, logs, configuration, sample items, policies, procedures, diagrams), on-site or virtual observations, (optionally) utilization of the work of others (as described elsewhere in this report), and (optionally) reperformance of controls.

Each requirement in the HITRUST CSF contains one or more evaluative elements. For example, requirement 0322.09u2Organizational.12, which reads "Media is encrypted when onsite unless physical security can be guaranteed, and always when offsite.", contains the following two evaluative elements: "1. The organization restricts the use of writable, removable media in organizational systems." and "2. The organization restricts the use of personally owned, removable media in organizational systems". The implementation and operation of all evaluative elements associated with applicable HITRUST CSF

requirements included in the assessment was evaluated by the external assessor in reaching an implementation score.

HITRUST developed a scoring rubric that is used by External Assessors to determine implementation scoring in a consistent and repeatable way by evaluating both implementation strength and implementation coverage, described as follows:

- The HITRUST CSF requirement's implementation strength is evaluated using a 5-point scale (tier 0 through tier 4) by considering the requirement's implementation and operation across the assessment scope, which consists of all organizational and system elements, including the physical facilities and logical systems / platforms, within the defined scope of the assessment.

- The HITRUST CSF requirement's implementation coverage is evaluated using a 5-point scale (very low through very high) by considering the percentage of the requirement's evaluative elements implemented and operating within the scope of the assessment.

The implementation scoring model utilized on e1 assessments incorporates the following scale. The overall score for each HITRUST CSF requirement ranges from 0 to 100 points in quarter increments based directly on the requirement's implementation score.

Implementation Score	Description	Points Awarded
Not Compliant (NC)	Very few if any of the evaluative elements in the HITRUST CSF requirement are implemented within the scope of the assessment. Rough numeric equivalent of 0% (point estimate) or 0% to 10% (interval estimate).	0
Somewhat Compliant (SC)	Some of the evaluative elements in the HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 25% (point estimate) or 11% to 32% (interval estimate).	25
Partially Compliant (PC)	About half of the evaluative elements in the HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 50% (point estimate) or 33% to 65% (interval estimate).	50
Mostly Compliant (MC)	Many but not all of the evaluative elements in HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 75% (point estimate) or 66% to 89% (interval estimate).	75
Fully Compliant (FC)	Most if not all of the evaluative elements in the HITRUST CSF requirement are implemented within the scope of the assessment, as validated through inspection of supporting evidence or utilization of the work of others. Rough numeric equivalent of 100% (point estimate) or 90% to 100% (interval estimate).	100

HITRUST

Scope of the Assessment

Company Background

Chinstrap Penguin Corp is a manufacturer, retailer and distributor of widgets for use in the care, feeding and housing of all Antarctic Chinstrap Penguins. Chinstrap Penguin Corp was established in 2005 and has grown to one of the largest widget producers in the world and now offers a number of specialized widgets to its customers and third-party distributors. In 2014 Chinstrap Penguin Corp entered the gadget market by acquiring Gadget Group and is now the third largest gadget manufacturer in the United States.

In-Scope Platform

The following table describes the platform that was included in the scope of this assessment.

Customer Central (a.k.a. "Portal")	
Description	The Portal is a platform that allows numerous applications and service offerings to be accessed by customers via a single web-based interface via a browser. It does this for numerous customers and allows their customers to obtain information in a single location. Chinstrap Penguin personnel access the Portal through a secure VPN to a bastion host. From the bastion host systems administrators connect via VDI to an administrative console for management of all in-scope applications and supporting infrastructure. The Portal is developed by Chinstrap Penguin personnel. It is built in Java and .Net. The solution leverages VMWare for scalability. The applications/service offerings that make up the Portal are Penguin Nest, Penguin Analytics, and South Pole Benefit Eligibility. Penguin Nest is an application that delivers content and applications from customer systems via the Portal. The application collects and feeds critical metrics to Penguin Analytics. Penguin Analytics is an application that delivers reporting and analytics capability to customers. It allows them to develop dashboards and reports and track KPIs with their information that is stored within the Portal. South Pole Benefits Eligibility allows our customers to provide benefit eligibility information so that users of the system have a single place to go to get the eligibility information from multiple customers. Meta data from the application is fed to Penguin Analytics for further analysis by customers.
Application(s)	Penguin Nest, Penguin Analytics, South Pole Benefits Eligibility
Database Type(s)	Oracle
Operating System(s)	HP-UX

Customer Central (a.k.a. "Portal")	
Residing Facility	Pelican Data Center
Exclusion(s) from scope	None

In-Scope Facilities

The following table presents the facilities that were included in the scope of this assessment.

Facility Name	Type of Facility	Third-party Managed?	Third-party Provider	City	State	Country
CP Framingham Manufacturing Facility	Office	No	-	Framingham	MA	United States of America
CP Headquarters and Manufacturing	Office	No	-	Las Vegas	NV	United States of America
Pelican Data Center	Data Center	Yes	Pelican Hosting	Salt Lake City	UT	United States of America

Services Outsourced

The following table presents outsourced services relevant to the scope of this assessment. The "Consideration in this Assessment" column of this table specifies the method utilized for each service provider relevant to the scope of this e1 assessment. Organizations undergoing e1 assessments have two options of how to address situations in which a HITRUST CSF requirement is fully or partially performed by a service provider (e.g., by a cloud service provider):

- The Inclusive method, whereby HITRUST CSF requirements performed by the service provider are included within the scope of the assessment and addressed through full or partial inheritance, reliance on third-party assurance reports, and/or direct testing by the external assessor, and

- The Exclusive (or Carve-out) method, whereby HITRUST CSF requirements performed by the service provider are excluded from the scope of the assessment and marked N/A with supporting commentary explaining that the HITRUST CSF requirement is fully performed by a party other than the assessed entity (for fully outsourced controls) or through commentary explaining the excluded partial performance of the HITRUST CSF requirement (for partially outsourced controls).

Third-party Provider	Relevant Service(s) Provided	Consideration in this Assessment
Pelican Hosting	Pelican Hosting provides a colocation facility where Chinstrap maintains a dedicated cage. Pelican Hosting personnel do not have logical access to any in-scope systems.	Included

HITRUST

Use of the Work of Others

For certain portions of the assessment and as allowed by HITRUST's Assurance Program requirements, the external assessor may have utilized the work of other assessors, auditors, and/or inspectors in lieu of direct testing. All assessment Use of the Work of Others, including those where the external assessor utilized the work of others, were subject to HITRUST's quality assurance review procedures. The table below details assessments utilized by the external assessor.

Potential options available for using the work of others allowed by HITRUST's Assurance Program Requirements include the following and are reflected in the "Utilization Approach" column of the below table if leveraged in this assessment:

- Inheritance of results from or reliance on another HITRUST validated assessment,
- Reliance on a recent third-party assurance report, and/or
- Reliance on testing performed by the assessed entity (i.e., by internal assessors).

Assessment Utilized	Assessed Entity	Assessment Type	Utilization Approach	Relevant Platforms	Relevant Facilities	Assessment Domains
Pelican Hosting HITRUST r2	Pelican Hosting	HITRUST r2	Inheritance	(All in-scope platforms)	(All in-scope facilities)	(All assessment domains)

HITRUST

Limitations of Assurance

Relying parties should consider the following in its evaluation of the findings in this report:

- This Insights Report provides transparency into the current state of HIPAA coverage and control maturity within the scoped environment for the Organization as described in the 'Coverage and Reportability' section above. This Insights Report supports the Organization in communicating the status of controls supporting HIPAA compliance and is not a certification of HIPAA compliance.

- This Insights Report accompanies a HITRUST CSF e1 Validated assessment. The accompanying e1 Validated assessment was scoped and performed in accordance with the HITRUST Assurance Program requirements designed to measure and report on control maturity for purposes of issuing HITRUST validated assessment reports. Consequently:

    - HITRUST assessments are scoped based on a defined boundary inclusive of specified management systems, physical facilities and IT platforms. Therefore, the HITRUST assessment may be scoped differently than an assessment focused exclusively to evaluating HIPAA compliance across the entirety of the Organization. HIPAA requires the safeguarding of protected health information regardless of the residing facility or IT platform. Parties relying on this report should therefore evaluate the Scope in relation to the Organization's HIPAA obligations in consultation with the Organization.

    - The nature, timing, and extent of the procedures performed by the HITRUST External Assessor Organization may differ from those performed in an assessment dedicated exclusively to evaluating HIPAA compliance and were not designed to specifically detect all instances of HIPAA non-compliance.

    - Compliance deficiencies noted in this report, if any, were identified through an evaluation of control maturity of the HITRUST CSF requirements mapping to HIPAA included in the Organization's HITRUST validated assessment and not in observance of any other criteria specific to HIPAA standards/implementation specifications.

- Mappings produced by HITRUST to authoritative sources are performed utilizing the NIST OLIR Program methodology outlined in NIST Interagency Report 8278 and subjected to HITRUST's internal quality review process.

- No assessment of controls or compliance status provides total assurance or 100% protection against possible control failures and instances of non-compliance. Because of their nature, controls may not prevent, or detect and correct, all errors or omissions relevant to compliance with regulatory statutes.

HITRUST

HIPAA Overview

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 is a US federal healthcare law. It applies to covered entities-doctors' offices, hospitals, health insurers, and other healthcare companies-with access to patients' protected health information (PHI), as well as to business associates, such as cloud service and IT providers, that process PHI on their behalf.

HIPAA, also known as Public Law 104-191, had two main purposes: to provide continuous health insurance coverage for workers who lose or change their job and to ultimately reduce the cost of healthcare by standardizing the electronic transmission of administrative and financial transactions. Other goals included combating abuse, fraud and waste in health insurance and healthcare delivery, and improving access to long-term care services and health insurance.

While its initial function primarily focused on regulating the health insurance industry, the act also allowed the United States Department of Health and Human Services (HHS) to set standards for the safeguarding of identifiable health information by legitimizing and protecting an individual's rights to their healthcare information as well as seeking to increase the efficiency and effectiveness of the healthcare industry as a whole. The scope of the law was later defined and expanded via the passage of the Privacy Rule, Security Rule, HITECH Act, and other expansions of the original HIPAA law.

The act contains five titles, or sections, in total:

- Title I protects coverage of health insurance for those who have changed or lost their jobs. It prevents group health plans from refusing to cover individuals who have pre-existing diseases or conditions and prohibits them from setting limits for lifetime coverage.

- Title II standardizes the processing of electronic healthcare transactions nation-wide. It requires the organizations to implement safe electronic access to the patients' health data, remaining in compliance with the privacy regulations which were set by the HHS.

- Title III relates to provisions which are tax-related, and general medical care guidelines.

- Title IV defines a further reform in health insurance, including provisions for those who have pre-existing diseases or conditions, and individuals who are seeking continued coverage.

- Title V includes provisions associated with company-owned insurance, and treatment of those who lost their citizenship for income tax reasons.

Adhering to HIPAA Title II is what is most often meant through the term "HIPAA compliance". Also known as the Administrative Simplification provisions, Title II includes the following HIPAA compliance requirements:

- National Provider Identifier Standard. Each healthcare entity, including individuals, employers, health plans and healthcare providers, must have a unique 10-digit National Provider Identifier number, or NPI.

- Transactions and Code Sets Standard. Healthcare organizations must follow a standardized mechanism for electronic data interchange (EDI) in order to submit and process insurance claims.

- HIPAA Enforcement Rule. This rule establishes guidelines for investigations into HIPAA compliance violations.

- HIPAA Privacy Rule. Officially known as the Standards for Privacy of Individually Identifiable Health Information, this rule establishes national standards to safeguard protected health information (PHI).

- HIPAA Security Rule. The Security Standards for the Protection of Electronic Protected Health Information (ePHI) sets standards for patient data security.

- HIPAA Breach Notification Rule. Officially titled, "Notification in the Case of Breach of Unsecured Protected Health Information", this requires covered entities to notify various parties when unsecured protected heath information (PHI) is impermissibly used or disclosed-or "breached,"-in a way that compromises the privacy and security of the PHI.

HITRUST

HIPAA Coverage and Reportability

The HITRUST validated assessment underlying this Insights Report provides evidence that specific HITRUST CSF control requirements mapping to portions of HIPAA have been implemented and to what degree, and also identifies relevant gaps in implementation. The HITRUST CSF, the inherent mappings to HIPAA as a supported authoritative source, and HITRUST's comprehensive assurance program can serve as important tools for organizations with HIPAA compliance obligations.

To learn about how HITRUST assessments support HIPAA compliance, see https://hitrustalliance.net/content/uploads/HITRUST-and-HIPAA.pdf.

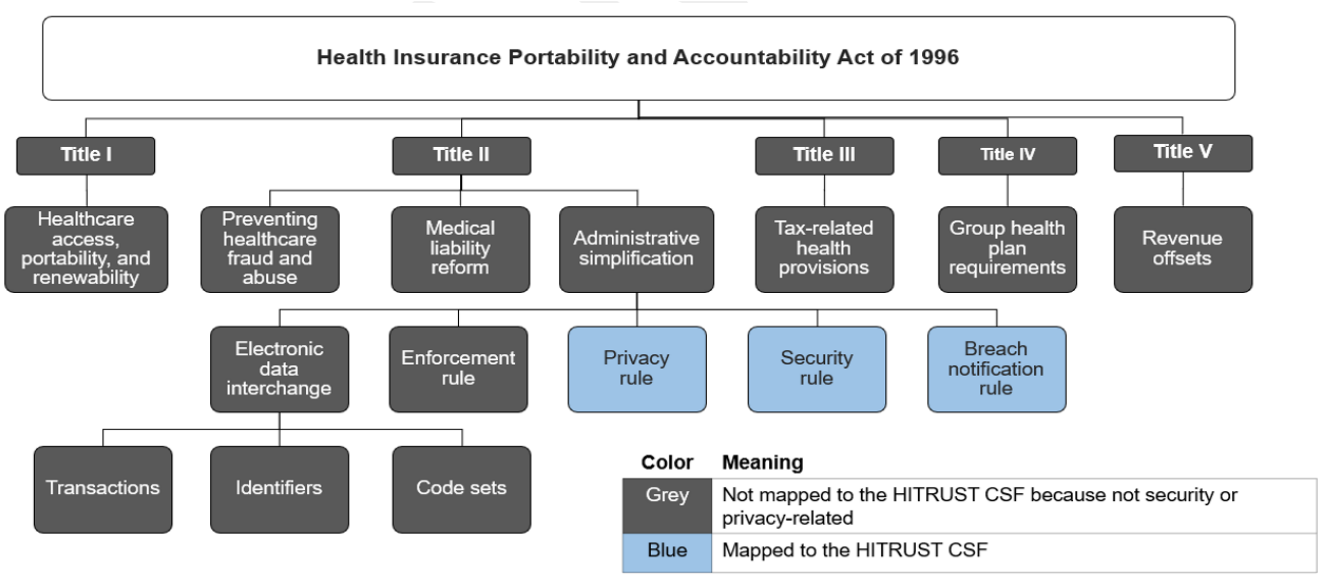
The following factors collectively determine the degree of HIPAA coverage and reportability in a HITRUST assessment:

- HITRUST's approach to incorporating HIPAA into the HITRUST CSF
- The Organization's assessment type selection, HITRUST CSF version selection, and assessment tailoring
- Characteristics of the Organization (e.g., covered entity)

Approach to incorporating HIPAA into the HITRUST CSF

The HITRUST CSF is composed exclusively of information security and privacy controls, and the scope of HIPAA extends far beyond just the security and privacy of protected health information. Therefore, HITRUST assessments do not evaluate coverage of or compliance with HIPAA in its entirety. HITRUST has incorporated into the HITRUST CSF the security and privacy-related aspects of HIPAA, specifically portions of 45 CFR Part 164 subparts C, D, and E.

The HITRUST CSF's coverage of HIPAA at a high level is as follows:



Further, the following portions the HIPAA Privacy Rule, Breach Notification Rule, and Security Rule were intentionally not incorporated into the HITRUST CSF:

- Sections dedicated only to outlining who must comply with the HIPAA Privacy Rule, Breach Notification Rule, and Security Rule:
  - 45 CFR Part 164 Subpart A, General Provisions
  - §164.302, Applicability [of the HIPAA Security Rule]
  - §164.400, Applicability [of the HIPAA Breach Notification Rule]
  - §164.500, Applicability [of the HIPAA Privacy Rule]
- Sections dedicated only to defining HIPAA's unique terminology:
  - §164.304, Definitions [in the HIPAA Security Rule]
  - §164.402, Definitions [in the HIPAA Breach Notification Rule]
  - §164.501, Definitions [in the HIPAA Privacy Rule]

Impact of assessment preferences and tailoring on HIPAA coverage and reportability

HITRUST assessments are performed against a subset of HITRUST CSF's numerous requirements. The requirements included in the accompanying HITRUST Essentials, 1-year (e1) assessment have been tailored based on the unique risks and compliance needs of the Organization and on the HITRUST CSF version selected by the Organization (v11.6.0).

Through tailoring, organizations can optionally add authoritative sources into their e1 assessments. When this occurs, the assessment is expanded to consider additional requirements mapping to the information security and/or privacy-related portions of the included authoritative sources. The resulting, tailored HITRUST e1 assessment then serves to directly

evaluate the Organization's adherence to a subset of the HITRUST CSF and indirectly evaluate the assessed entity's compliance with the information security and/or privacy aspects of the included authoritative source(s).

The HITRUST CSF is constantly updated by HITRUST in response to changes in the cybersecurity threat landscape and updates to included authoritative sources. Organizations can utilize the most recent HITRUST CSF version in HITRUST e1 assessments. As HITRUST advances the framework, more and better reporting capabilities are unlocked. Not all versions allow for the HITRUST Compliance Insights reporting against all portions of HIPAA. Compliance Insights Reports support for each HIPAA rule by CSF version is as follows:

- HIPAA Breach Notification Rule: HITRUST CSF v11.0.0 and later
- HIPAA Privacy Rule: HITRUST CSF v11.0.0 and later
- HIPAA Security Rule: HITRUST CSF v9.5.0 and later

The impact of the Organization's assessment tailoring and HITRUST CSF version selection on HIPAA coverage and reporting is as follows:

HIPAA Privacy Rule	HIPAA Breach Notification Rule	HIPAA Security Rule

Color	Meaning
Light blue	Included in this HITRUST assessment and in this HIPAA Insights Report
Grey	Excluded from this HITRUST assessment by the Organization through assessment tailoring, and not included in this HIPAA Insights Report as a result

The Organization did not configure the accompanying HITRUST e1 assessment to include consideration of the HIPAA Breach Notification Rule or the HIPAA Privacy Rule. However, the Organization is still required to comply with aspects of the HIPAA Breach Notification Rule and the HIPAA Privacy Rule as a result of their "Business Associate" designation. Parties seeking to understand more about the Organization's compliance with the HIPAA Breach Notification Rule and the HIPAA Privacy Rule should consult with the Organization.

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. The Security Rule's "addressable" implementation specifications are inherently considered in the HITRUST assessment underlying this HIPAA Insights Report.

HITRUST

Organizational characteristics impacting HIPAA applicability and coverage

HIPAA's Security Rule, Breach Notification Rule, and Privacy Rule all contain standards and implementation specifications applicable only to certain types of organizations. Several standards and implementation specifications apply only to covered entities, some apply only to business associates, while others apply only to group health plans.

Specific to the HITRUST assessment scope, characteristics affecting the applicability of HIPAA standards and implementation specifications considered in the HITRUST e1 assessment underlying this HIPAA Insights Report are as follows:

Entity Type	Business Associate
Group Health Plan?	No

HITRUST

Appendix A: HIPAA-relevant Observations

During the HITRUST assessment accompanying this HIPAA Insights Report, the implemented control maturity level on each of the following HITRUST CSF requirements scored less than "Fully Compliant". These conditions were identified as relevant to the Organization's HIPAA compliance efforts, as each of these HITRUST CSF requirements map to one or more HIPAA requirements. The relying party should evaluate these items (and the associated risk treatment) in consultation with the Organization.

HIPAA Security Rule - Subpart C — Security Standards for the Protection of Electronic Protected Health Information

Reference	Mapped HITRUST CSF Requirement	Maturity level(s) scoring less than fully compliant	Management's stated corrective actions (unvalidated)
164.308(a)(1)(i), 164.308(a)(1)(ii)(B), 164.308(a)(4)(ii)(C)	Mapped BUID: 0104.02a1Organizational.12 / CVID: 0297.0. Policies and/or standards related to user roles and responsibilities include: implementing and acting in accordance with the organization's information security policies; protecting assets from unauthorized access, disclosure, modification, destruction, or interference; executing particular security processes or activities; ensuring responsibility is assigned to the individual for actions taken; reporting security events or potential events or other security risks to the organization; and security roles and responsibilities are defined and clearly communicated to users and job-candidates during the pre-employment process.	Implemented	No corrective action plans were communicated to HITRUST for this condition.

This section has been truncated for this sample report

HITRUST

Appendix B: Relevant HITRUST Assessment Results and Mappings

Below are the assessment results and control maturity evaluations for each assessed HITRUST CSF requirement mapped to the areas of HIPAA considered in the underlying HITRUST CSF assessment, organized by HIPAA part.

This section also shows the HITRUST CSF requirements mapped by HITRUST to each considered HIPAA standard/implementation specification. Note that many more mappings exist between HIPAA and the HITRUST CSF; this section lists only the mapping subset relevant to the underlying HITRUST assessment as determined through the factors described in the HIPAA Coverage and Reportability section of this document.

In addition to HIPAA, the HITRUST CSF is mapped to dozens of additional authoritative sources, enabling a wide range of compliance coverage within HITRUST Assessments. Mappings produced by HITRUST are performed utilizing the NIST OLIR Program methodology outlined in NIST Interagency Report 8278. These mappings were created by HITRUST and have undergone HITRUST's internal quality review process consisting of at least five of review before being finalized: automated review, initial mapper review, peer review, management review, and quality assurance review. Questions about these mappings should be routed to HITRUST's Support team.

Note that one or more HIPAA standards/implementation specifications were intentionally omitted from this section due to their inapplicability to the Organization and/or lack of coverage in the underlying HITRUST CSF assessment—these HIPAA standards/implementation specifications are, however, shown in the "HIPAA Scorecard" section of this document.

HIPAA Security Rule

HITRUST CSF Requirement	Implemented Score
164.308 - Administrative Safeguards	
164.308(a)(1)(i) - A covered entity or business associate must, in accordance with §164.306: Implement policies and procedures to prevent, detect, contain, and correct security violations.	

HITRUST

HITRUST CSF Requirement	Implemented Score
Mapped BUID: 11966.01cNYDOHSystem.5 / CVID: 2039.0. The organization requires that users of information system accounts, or roles, with access to the following list of security functions or security-relevant information, use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for the following functions: (i) setting/modifying audit logs and auditing behavior; (ii) setting/modifying boundary protection system rules; (iii) configuring/modifying access authorizations (i.e., permissions, privileges); (iv) setting/modifying authentication parameters; and (v) setting/modifying system configurations and parameters.	Fully Compliant
Mapped BUID: 07901.10mSROrganizational.1 / CVID: 1961.0. Maintain and adhere to a documented process to remediate all critical, high, and medium risk security vulnerabilities promptly.	Fully Compliant
Mapped BUID: 15.10cNIST80053System.5 / CVID: 1277.0. The organization incorporates the detection of unauthorized security-relevant changes to the information system into the organization incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.	Fully Compliant
Mapped BUID: 0625.10c2System.8 / CVID: 1279.0. The organization employs integrity verification tools to detect unauthorized, security-relevant configuration changes to software and information.	Fully Compliant
Mapped BUID: 06185.09bNYDOHSystem.10 / CVID: 2157.0. The organization takes actions to verify that the provisioned security function implementation being assessed and/or monitored meets security function requirements and is an approved system configuration.	Fully Compliant
Mapped BUID: 0165.05a3Organizational.3 / CVID: 0451.0. The organization publishes security guidelines and/or daily operational procedures relating to processes that complement, clarify, and enforce security policies.	Fully Compliant
Mapped BUID: 06184.09bNYDOHSystem.5 / CVID: 2156.0. The organization continuously monitors and evaluates the system's security functions to ensure they are operating as intended and changes do not have an adverse effect on system performance.	Fully Compliant

HITRUST

HITRUST CSF Requirement	Implemented Score
Mapped BUID: 1438.09e2System.4 / CVID: 0841.0. The service provider protects the company's data with reasonable controls (e.g., policies and procedures) designed to detect, prevent, and mitigate risk.	Fully Compliant
Mapped BUID: 1443.09fCMSSystem.1 / CVID: 0852.0. The organization employs defined processes, methods, and techniques (defined in the applicable security plan) to monitor security control compliance by external service providers on an ongoing basis.	Fully Compliant
Mapped BUID: 1561.11c1Organizational.4 / CVID: 1488.0. The organization implements an incident handling capability for security incidents that includes detection and analysis, containment, eradication, and recovery (including public relations and reputation management). Components of the incident handling capability include: a policy (setting corporate direction); procedures defining roles and responsibilities; incident handling procedures (business and technical); communication; reporting and retention; and references the organization's vulnerability management program elements (e.g., IPS, IDS, forensics, vulnerability assessments, validation).	Fully Compliant
Mapped BUID: 0104.02a1Organizational.12 / CVID: 0297.0. Policies and/or standards related to user roles and responsibilities include: implementing and acting in accordance with the organization's information security policies; protecting assets from unauthorized access, disclosure, modification, destruction, or interference; executing particular security processes or activities; ensuring responsibility is assigned to the individual for actions taken; reporting security events or potential events or other security risks to the organization; and security roles and responsibilities are defined and clearly communicated to users and job-candidates during the pre-employment process.	Mostly Compliant

This section has been truncated for this sample report

HITRUST

Appendix C: HITRUST Background

HITRUST Alliance, Inc. was born out of the belief that information security should be a core pillar of, rather than an obstacle to, the broad adoption of information systems and exchanges. HITRUST®, in collaboration with industry, business, technology and information security leaders, established the HITRUST CSF, a certifiable framework that can be used by any and all organizations that create, access, store or exchange personal, sensitive, and/or financial information.

Beyond the establishment of the HITRUST CSF®, HITRUST is also driving the adoption of and widespread confidence in the framework and sound risk management practices through awareness, education, advocacy, and other outreach activities.

An integral component to achieving HITRUST's goal to advance the protection of sensitive information is the establishment of a practical mechanism for validating an organization's compliance with the HITRUST CSF.

The HITRUST CSF is an overarching security framework that incorporates and leverages the existing security requirements placed upon organizations, including international (GDPR, ISO), federal (e.g., FFIEC, HIPAA and HITECH), state, third party (e.g., PCI and COBIT), and other government agencies (e.g., NIST, FTC, and CMS). The HITRUST CSF is already being widely adopted by leading organizations in a variety of industries as their information protection framework.

HITRUST has developed the HITRUST Assurance Program, which encompasses the common requirements, methodology and tools that enable both an organization and its business partners to take a consistent and incremental approach to managing compliance.

The HITRUST Assurance Program is the mechanism that allows organizations and their business partners and vendors to assess and report against multiple sets of requirements. Unlike other programs, the oversight, vetting, and governance provided by HITRUST and the HITRUST Assessor Council affords greater assurances and security across all industries.

To learn about how HITRUST supports HIPAA compliance efforts, visit https://hitrustalliance.net/hitrust-for-hipaa/. For more information about HITRUST, the HITRUST CSF and other HITRUST offerings and programs, visit https://hitrustalliance.net.