HITRUST

HIPAA Insights

Based upon a HITRUST Risk-based, 2-year (r2) Validated Assessment

Chinstrap Penguin Corporation

As of February 10, 2023

SAMPLE FOR ILLUSTRATIVE USE ONLY

HITRUST

Contents

HITRUST

1. Transmittal Letter

February 10, 2023

Chinstrap Penguin Corporation
123 Main Street
Anytown, TX 12345

Through HITRUST's "Assess Once, Report Many" capability made possible through the HITRUST CSF, HITRUST has prepared this HIPAA Compliance Insights Report at the request of Chinstrap Penguin Corp. ("the Organization"). This Insights Report contains detailed information relating to the coverage and maturity of controls supporting the Organization's compliance with aspects of HIPAA for the scope outlined below, based on control validation procedures executed during a HITRUST Risk-based, 2-year (r2) Validated Assessment using v11.0.0 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 r2 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 r2 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

Facility:

- CP Framingham Manufacturing Facility (Other) located in Framingham, Massachusetts, United States of America
- CP Headquarters and Manufacturing (Office) located in Las Vegas, Nevada, United States of America

- Pelican Data Center (Data Center) managed by Pelican Hosting located in Salt Lake City, Utah, 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 Risk-based, 2-year (r2) Validated Assessment, the Organization asserted that management of the Organization:

- Is responsible for the implementation of information protection controls.
- Has made available to the HITRUST External Assessor all records and necessary documentation related to the information protection controls included within the scope of the Risk-based, 2-year (r2) Validated Assessment.
- 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 Risk-based, 2-year (r2) 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 Risk-based, 2-year (r2) 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.

HITRUST

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 the maintenance of the HITRUST CSF and HITRUST Assurance Program against which the Organization and an Authorized HITRUST External Assessor completed this assessment.

HITRUST is also responsible for producing the mappings from various authoritative sources, including HIPAA, to the HITRUST CSF. Information about HITRUST's "Assess Once, Report Many" approach and 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 this report's Limitations of Assurance section.

HITRUST

HITRUST

2. HIPAA Insights Scorecard

The tables below provide insights on HIPAA compliance for the environment assessed. Each HIPAA standard and implementation specification listed is assigned a compliance score for the policy, procedure, and implemented control maturity levels. Note that 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. The compliance scores are based on the assessment results of the HITRUST CSF requirement(s) as mapped to the HIPAA standard or implementation specification.

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.

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

MC	Mostly 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 66 - 89.99%.
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

Security Rule

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

Reference	Standard or Implementation Specific Title	Policy Scoring	Procedure Scoring	Implemented Scoring
164.308(a)(7)(ii)(D)	Testing and revision procedures	MC	MC	MC
164.308(a)(7)(ii)(E)	Applications and data criticality analysis	FC	FC	FC
164.308(a)(8)	Evaluation	FC	FC	FC
164.308(b)(1)	Business associate contracts and other arrangements	Does Not Apply (only applies to covered entities)		
164.308(b)(2)	Business associate contracts and other arrangements	FC	FC	FC
164.308(b)(3)	Written contract or other arrangement	FC	FC	FC
Security Rule: § 164.310 Physical safeguards				
164.310(a)(1)	Facility access controls	FC	FC	FC
164.310(a)(2)(i)	Contingency operations	FC	FC	FC
164.310(a)(2)(ii)	Facility security plan	FC	FC	FC
164.310(a)(2)(iii)	Access control and validation procedures	FC	FC	FC
164.310(a)(2)(iv)	Maintenance records	FC	FC	FC
164.310(b)	Workstation use	FC	FC	FC
164.310(c)	Workstation security	FC	FC	FC
164.310(d)(1)	Device and media controls	FC	FC	FC
164.310(d)(2)(i)	Disposal	FC	FC	FC
164.310(d)(2)(ii)	Media re-use	FC	FC	FC
164.310(d)(2)(iii)	Accountability	MC	MC	MC
164.310(d)(2)(iv)	Data backup and storage	FC	FC	FC

Section 6 has been truncated for this sample report

HITRUST

3. Assessment Context

The assessed entity completed the following tailoring questionnaire to derive this assessment's customized set of HITRUST CSF requirements based on organizational, geographical, technical, and regulatory risk factors.

Assessment Type
HITRUST Risk-based, 2-year (r2) Validated Assessment

General Risk Factors	
Entity Type	Healthcare - Business Associate
Do you offer Infrastructure as a Service (IaaS)?	No
Organization Type	Service Provider (Information Technology, IT)

Technical Risk Factors	
Does the organization allow personally owned devices to connect to scoped organizational assets (i.e., BYOD - bring your own device)?	Yes
Is any aspect of the scoped environment hosted on the cloud?	Yes
Is scoped information sent by the organization using courier services, internal mail services, or external mail services (e.g., USPS)?	No - We do not send scoped information using courier services both internal and external mail services.
Does the organization perform information systems development (either in-house or outsourced) for any scoped system, system service, or system component?	Yes
Does the scoped environment allow dial-up/dial-in capabilities (i.e., functional analog modems)?	No - The scoped environment does not allow the use of modems or dial-up connection. All employees connect to a VPN.
Does the organization allow the use of electronic signatures to provide legally binding consent within the scoped environment, e.g., simple or basic electronic signatures (SES), advanced electronic or digital signature (AES), or qualified advanced electronic or digital signatures (QES)?	No - We do not make use of electronic signatures.
Does the system allow users to access the scoped environment from an external network that is not controlled by the organization?	Yes

Is scoped information sent and/or received via fax machine (i.e., an actual machine, excluding efax or scan to email)?	No - No actual fax machines used in the system.
Does the organization use any part of the scoped systems, system components, or system services to sell goods and/or services?	No - We do not use any of its scoped systems to sell any products or services to end users. The application has no feature which enables the selling of products or services.
Is the system(s) accessible from the Internet?	Yes
Number of interfaces to other systems	Fewer than 25
Number of transactions per day	6,750 to 85,000
Number of users of the system(s)	Greater than 5,500
Is the system(s) publicly positioned?	No - The system is not available to the public. Only authorized employees and dependents can access the system. No kiosks are in use.
Is the scoped system(s) (on-premises or cloud-based) accessible by third-party personnel (e.g., business partners, vendors, cloud providers)?	Yes
Does the system(s) transmit or receive data with a third-party?	No - We do not transmit or receive data from third-parties.
Are hardware tokens used as an authentication method within the scoped environment?	No - We do not use hardware tokens; we use an authenticator application.
Do any of the organization's personnel travel to locations the organization deems to be of significant risk?	No - Our personnel do not travel to high-risk locations.
Are wireless access points in place at any of the organization's in-scope facilities?	No - There are no wireless access points in place at any of the organization's in-scope facilities

Compliance Factors (Optional)
CCPA
HIPAA Security Rule

HITRUST

4. 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 describe 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.

Customer Central (a.k.a. "Portal")	
Application(s)	Penguin Nest, Penguin Analytics, South Pole Benefits Eligibility
Database Type(s)	Oracle
Operating System(s)	HP-UX
Residing Facility	Pelican Data Center
Exclusion(s) from scope	Content and applications from customer systems that are delivered via the Portal are outside the scope of this assessment. This includes customers who choose to leverage the embedded credit card processing page, which is offered as an add-on service. The embedded credit processing page is provided and managed by a third-party service provider.

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	Other	No	(None)	Framingham	Massachusetts	United States of America
CP Headquarters and Manufacturing	Office	No	(None)	Las Vegas	Nevada	United States of America
Pelican Data Center	Data Center	Yes	Pelican Hosting	Salt Lake City	Utah	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 r2 assessment. HITRUST requires the inclusive method must be used on HITRUST r2 validated assessments. Under the Inclusive method, 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.

Third-party Provider	Relevant Service(s) Provided	Consideration in this Assessment
Seashore Offsite Data Storage	Seashore provides backup tape delivery and storage in a secure offsite facility. No customer, covered, otherwise confidential information is stored at Seashore's facilities, however.	Included
Pelican Hosting	Pelican Hosting provides a colocation facility where Chinstrap Penguin maintains a dedicated cage. Pelican Hosting personnel do not have logical access to any in-scope systems.	Included

5. Use of the Work of Others

An Authorized HITRUST External Assessor Organization (i.e., the external assessor) performed procedures to validate the Organization's asserted control maturity scores. These validation procedures were designed by the external assessor based upon the assessment's scope in observance of HITRUST's Assurance Program Requirements and consisted of inquiry with key personnel, inspection of system-generated evidence (e.g., access lists, logs, configurations, sample items), on-site or virtual observations, and (optionally) reperformance of controls.

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 procedures performed by the external assessor, 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 Organization (i.e., by internal assessors).

Assessment Utilized	Assessed Entity	Assessment Type	Report Date(s)	Utilization Approach	Relevant Platforms	Relevant Facilities	Assessment Domains
Pelican Hosting HITRUST r2	Pelican Hosting	HITRUST r2	7/29/22	Inheritance	(All in-scope platforms)	(All in-scope facilities)	(All assessment domains)

6. Limitations of Assurance

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

- This HIPAA 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 HIPAA Coverage section above. This report therefore supports the Organization communicating the status of controls supporting HIPAA Compliance and is not a certification of HIPAA Compliance.

- This HIPAA Insight report accompanies a HITRUST CSF r2 validated assessment. The accompanying r2 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 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 requirements.

- Mappings produced by HITRUST to authoritative sources are performed utilizing the NIST OLIR Program methodology outlined in NISTIR 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.

7. 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.

8. Coverage and Reportability

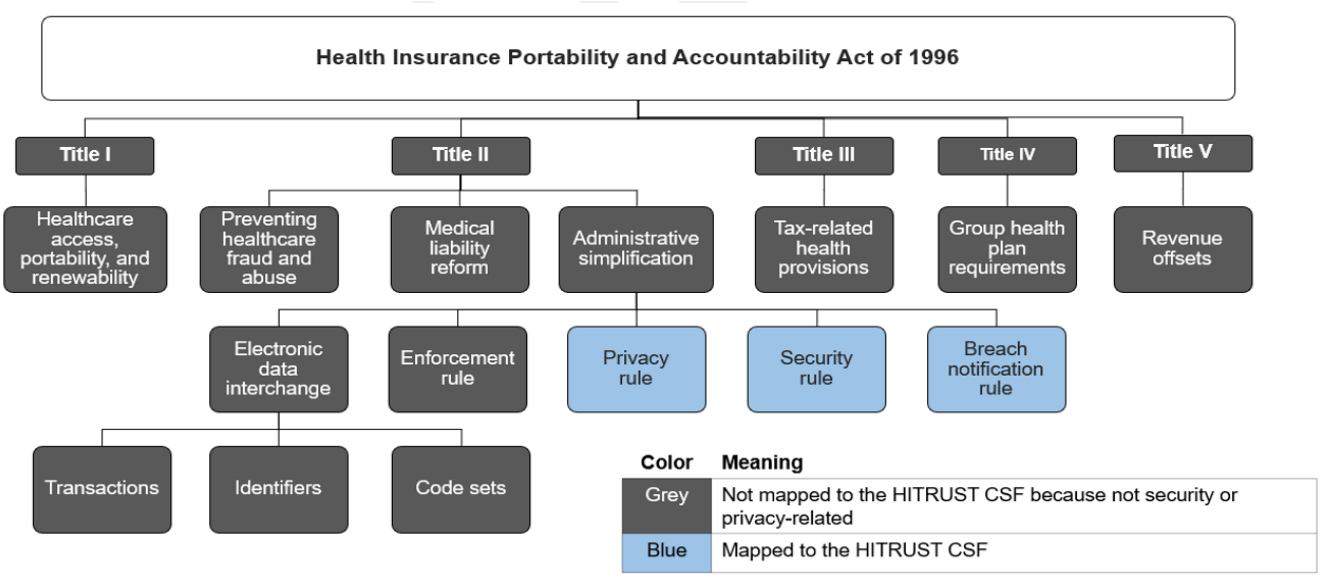
A HITRUST validated assessment provides evidence that specific HITRUST CSF control requirements that map to HIPAA Standards and Implementation Specifications have been implemented, measures how well they have been implemented, and documents the nature and volume of any identified gaps in implementation. To learn about how HITRUST assessments support HIPAA compliance, see https://hitrustalliance.net/content/uploads/HITRUST-and-HIPAA.pdf. The HITRUST CSF, the inherent mapping to HIPAA as a supported authoritative source, and the robust and comprehensive security assurance program are important tools for Covered Entities and Business Associates with HIPAA compliance obligations. The following factors collectively determine the degree of HIPAA coverage 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., business associate or 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 Risk-based, 2-year (r2) assessment have been tailored to the unique risks and compliance needs of the Organization and on the HITRUST CSF version selected by the Organization (v11.0.0).

Through tailoring, organizations can optionally add authoritative sources into their r2 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 r2 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 r2 assessments or can optionally utilize one of many prior HITRUST CSF versions. As HITRUST advances the framework, more and better reporting capabilities are unlocked. Not all versions allow for the HITRUST Insights reporting against all portions of HIPAA. Insights Reports support for each HIPAA rule by CSF version is as follows:

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

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

HIPAA Security Rule	HIPAA Breach Notification Rule	HIPAA Privacy 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, so also not included in this HIPAA Insights Report.

The Organization did not configure the accompanying HITRUST r2 assessment to include consideration of the HIPAA Breach Notification Rule or HIPAA Privacy Rule. However, the Organization is still required to comply with aspects of the HIPAA Breach Notification Rule and 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 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 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 r2 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 Validated Assessment accompanying this HIPAA Insights Report, the policy, process, and/or implemented control maturity levels 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 standards or implementation specifications. The relying party should evaluate these items (and the associated risk treatment—if specified) in consultation with the Organization.

Security Rule

Mapped HITRUST CSF Requirement	Maturity level(s) scoring less than fully compliant	Mappings to HIPAA Security Rule	Management's stated corrective actions (unvalidated)
BUID: 1105.09c1Organizational.2 / CVID: 0017.0. Access authorization (e.g., access requests, approvals, and provisioning) is segregated among multiple individuals or groups.	Policy, Procedure, Implemented	164.308(a)(3)(ii)(A)	*[Status: Not Started, Target Date: 9/15/2023]* We will add overt policy and procedure statements requiring the practice of segregating access 'requestors' from access 'approvers'. The implementation update is already in place; tickets in the 'Access Request' Jira project indicate a clear 'requestor' different than the clear 'approver'. (In progress, targeted for 2023-09-30)

Mapped HITRUST CSF Requirement	Maturity level(s) scoring less than fully compliant	Mappings to HIPAA Security Rule	Management's stated corrective actions (unvalidated)
BUID: 1105.09c1Organizational.2 / CVID: 0017.0. Access authorization (e.g., access requests, approvals, and provisioning) is segregated among multiple individuals or groups.	Policy, Procedure, Implemented	164.308(a)(4)(i), 164.308(a)(4)(ii)(B), 164.308(a)(4)(ii)(C)	*[Status: Not Started, Target Date: 9/15/2023]* We will add overt policy and procedure statements requiring the practice of segregating access 'requestors' from access 'approvers'. The implementation update is already in place; tickets in the 'Access Request' Jira project indicate a clear 'requestor' different than the clear 'approver'. (In progress, targeted for 2023-09-30)
BUID: 1334.02e2Organizational.12 / CVID: 0342.0. The organization ensures that the senior executives have been trained in their specific roles and responsibilities.	Implemented	164.308(a)(5)(i)	No corrective action plans were communicated to HITRUST for this observation.
BUID: 1015.01d2System.10 / CVID: 0074.0. Users acknowledge receipt of passwords.	Implemented	164.308(a)(5)(ii)(D)	No corrective action plans were communicated to HITRUST for this observation.
BUID: 0168.05b2Organizational.5 / CVID: 0459.0. Security plans are reviewed at least every three years (prior to the plans expiration), when changes are made to the information system or information protection requirements, or when incidents occur that impact the plans validity.	Policy, Procedure, Implemented	164.308(a)(6)(i), 164.316(b)(2)(iii)	No corrective action plans were communicated to HITRUST for this observation.

Appendix A 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 rule and section. To learn more about control maturity evaluation in HITRUST assessments, visit https://hitrustalliance.net/content/uploads/Evaluating-Control-Maturity-Using-the-HITRUST-Approach.pdf.

This section also shows the HITRUST CSF requirements mapped by HITRUST to each considered HIPAA standard and 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 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 are not reviewed by or endorsed by external regulatory bodies, and instead undergo at least five levels of internal HITRUST review before being finalized: automated review, initial mapper review, peer review, management review, and quality assurance review. Questions or concerns about these mappings should be routed to HITRUST's Support team.

Note that one or more HIPAA implementation specifications and/or standards 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 implementation specifications and/or standards are, however, shown in the "HIPAA Insights Scorecard" section of this document.

Security Rule

HITRUST CSF Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
Security Rule: § 164.308 Administrative safeguards			
164.308(a)(1)(i) - Security management process: Implement policies and procedures to prevent, detect, contain, and correct security violations.			

HITRUST CSF Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
BUID: 0113.04a2Organizational.1 / CVID: 0431.2. As applicable to the focus of a security policy particular document, security policies contain: the organization's mission, vision, values, objectives, activities, and purpose, including the organization's place in critical infrastructure; a definition of information security, its overall objectives and scope and the importance of security as an enabling mechanism for information sharing; a statement of management intent, supporting the goals and principles of information security in line with the business strategy and objectives; a framework for setting control objectives and controls, including the structure of risk assessment and risk management; the need for information security; the goals of information security; the organization s compliance scope; legislative, regulatory, and contractual requirements, including those for the protection of covered information and the legal and ethical responsibilities to protect this information; arrangements for notification of information security incidents, including a channel for raising concerns regarding confidentially, without fear of blame or recrimination; a definition of general and specific responsibilities for information security management, including reporting information security incidents; references to documentation which may support the policy (e.g., more detailed security policies and procedures for specific information systems or security rules users comply with); a brief explanation of the security policies, principles, standards, and compliance requirements of particular importance to the organization (including but not limited to CSF control objectives such as: (a) compliance with legislative, regulatory, and contractual requirements; (b) security education, training, and awareness requirements for the workforce, including researchers and research participants; (c) incident response and business continuity management; (d) consequences of information security policy violations; (e) continuous monitoring; (f) designating and maintaining an appropriately resourced and technically experienced information security team; (g) physical security of areas where sensitive information (e.g., PII, PCI and PMI data); and (h) coordination among organizational entities. As applicable to the focus of a security policy particular document, security policies also prescribe the development, dissemination, and review/update of formal, documented procedures to facilitate the implementation of security policy and associated security controls.	Fully Compliant	Fully Compliant	Fully Compliant
BUID: 0707.10b2System.1 / CVID: 1264.0. Applications which store, process or transmit covered information undergo automated (non-manual) application vulnerability testing with an emphasis on input validation controls at least annually by a qualified party.	Fully Compliant	Fully Compliant	Fully Compliant
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	Fully Compliant	Fully Compliant
BUID: 0113.04a1Organizational.2 / CVID: 0431.1. The organizations information security policy is developed, published, disseminated, and implemented. The information security policy documents: state	Fully Compliant	Fully Compliant	Fully Compliant

HITRUST CSF Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
the purpose and scope of the policy; communicate managements commitment; describe management and workforce members roles and responsibilities; and establish the organization's approach to managing information security.			
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.	Fully Compliant	Fully Compliant	Fully Compliant
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	Fully Compliant	Fully Compliant
BUID: 1438.09e2System.4 / CVID: 0841.0. The service provider protects the companys data with reasonable controls (e.g., policies and procedures) designed to detect, prevent, and mitigate risk.	Fully Compliant	Fully Compliant	Fully Compliant

164.308(a)(1)(ii)(A) - Risk analysis: Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.			
BUID: 1704.03b1Organizational.12 / CVID: 0394.0. The organization performs risk assessments that address all the major objectives of the HITRUST CSF. Risk assessments are consistent and identify information security risks to the organization. Risk assessments are to be performed at planned intervals and when major changes occur in the environment, and the results reviewed annually.	Fully Compliant	Fully Compliant	Fully Compliant

Appendix B 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.