HITRUST

PHIPA Insights

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

Chinstrap Penguin Corporation

As of February 26, 2024

SAMPLE FOR ILLUSTRATIVE USE ONLY

HITRUST

Contents

HITRUST

1. Transmittal Letter

February 26, 2024

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 Ontario Personal Health Information Protection Act ("PHIPA") Insights Report at the request of Chinstrap Penguin Corporation ("the Organization"). This Insights Report contains detailed information relating to the coverage and maturity of controls supporting the Organization's compliance with aspects of PHIPA for the scope outlined below, based on control validation procedures executed during a HITRUST Risk-based, 2-year (r2) Validated Assessment using v11.2.0 of the HITRUST CSF. The Organization can leverage this report to share information regarding their PHIPA 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 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.

Part V.1 of PHIPA requires healthcare organizations to conduct a risk assessment, specifically to "perform, for each system that retrieves, processes or integrates personal health information that is accessible by means of the electronic health record, an assessment with respect to, threats, vulnerabilities and risks to the security and integrity of the personal health information", as well as "an assessment with respect to, how each of those systems may affect the privacy of the individuals to whom the information relates". 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 § 55.3(10) of PHIPA.

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

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 PHIPA, 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.

HITRUST

HITRUST

2. PHIPA Scorecard

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

The Organization may have in place additional controls relevant to their PHIPA 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

SC	Somewhat Compliant: The control maturity level's scores across all HITRUST CSF requirements included in the Organization's HITRUST assessment mapped to the PHIPA requirement averaged 11 - 32.99%.
MC	Mostly Compliant: The control maturity level's scores across all HITRUST CSF requirements included in the Organization's HITRUST assessment mapped to the PHIPA requirement 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 PHIPA requirement 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 PHIPA coverage" sections of this document), the PHIPA requirement does not apply to the scoped aspects of the Organization.

HITRUST

Part II

Part II - Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
10.1(1): Electronic audit log				
10.1(1)(a)	Electronic audit log	Does Not Apply (for health information custodians only)		
10.1(1)(b)	Electronic audit log	Does Not Apply (for health information custodians only)		
10.1(1)(c)	Electronic audit log	Does Not Apply (for health information custodians only)		
10.1(4): Content of log				
10.1(4)(a)	Content of log	Does Not Apply (for health information custodians only)		
10.1(4)(b)	Content of log	Does Not Apply (for health information custodians only)		
10.1(4)(c)	Content of log	Does Not Apply (for health information custodians only)		
10.1(4)(d)	Content of log	Does Not Apply (for health information custodians only)		
10.1(4)(e)	Content of log	Does Not Apply (for health information custodians only)		
11(1): Accuracy				
11(1)	Accuracy	Does Not Apply (for health information custodians only)		
11(2): Accuracy - disclosure				
11(2)a	Accuracy - disclosure	Does Not Apply (for health information custodians only)		
11(2)b	Accuracy - disclosure	Does Not Apply (for health information custodians only)		
11.1: Steps to ensure collection				

Part II - Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
11.1	Steps to ensure collection	Does Not Apply (for health information custodians only)		
11.2(1): Limits on use of de-identified information				
11.2(1)	Limits on use of de-identified information	FC	MC	SC
12(1): Security				
12(1)	Security	Does Not Apply (for health information custodians only)		

This table has been truncated for this sample report

Part III

Part III - Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
18(1): Elements of consent				
18(1)(a)	Elements of consent	Does Not Apply (for health information custodians only)		
18(1)(b)	Elements of consent	Does Not Apply (for health information custodians only)		

This table has been truncated for this sample report

Part IV

Part IV - Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
29: Requirement for consent				

Part IV - Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
29(a)	Requirement for consent	Does Not Apply (for health information custodians only)		
29(b)	Requirement for consent	Does Not Apply (for health information custodians only)		
30(1): Other information				
30(1)	Other information	Does Not Apply (for health information custodians only)		
30(2): Extent of information				
30(2)	Extent of information	Does Not Apply (for health information custodians only)		
31(1): Use and disclosure of personal health information				
31(1)	Use and disclosure of personal health information	Does Not Apply (for health information custodians only)		

This table has been truncated for this sample report

Part V

Part V - Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
52(4): Home and community care service information				
52(4)	Home and community care service information	Does Not Apply (for health information custodians only)		
52(7): Duty of health information custodian				
52(7)	Duty of health information custodian	Does Not Apply (for health information custodians only)		
53(2): Detail in request				
53(2)	Detail in request	Does Not Apply (for health information custodians only)		

Part V - Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
53(3): Request for access				
53(3)	Request for access	Does Not Apply (for health information custodians only)		

This table has been truncated for this sample report

Part V.1

Part V.1 - Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
55.2(2): Functions of prescribed organization				
55.2(2)1	Functions of prescribed organization	Does Not Apply (for the prescribed organization only)		
55.2(2)2	Functions of prescribed organization	Does Not Apply (for the prescribed organization only)		
55.2(2)3	Functions of prescribed organization	Does Not Apply (for the prescribed organization only)		
55.2(2)4	Functions of prescribed organization	Does Not Apply (for the prescribed organization only)		
55.2(3): Other powers and duties				
55.2(3)	Other powers and duties	Does Not Apply (for the prescribed organization only)		

This table has been truncated for this sample report

HITRUST

Part VII

Part VII - Reference	Requirement	Policy Scoring	Procedure Scoring	Implemented Scoring
70: Non-retaliation				
70(a)	Non-retaliation	FC	MC	SC
70(b)	Non-retaliation	FC	MC	SC
70(c)	Non-retaliation	FC	MC	SC
70(d)	Non-retaliation	FC	MC	SC

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, technical, and regulatory risk factors. The Organization's responses to tailoring factor questions capture important risk considerations supporting an organization's overall risk analysis obligations and are considered alongside the Organization's performance of a risk analysis adhering to § 55.3(10) of PHIPA.

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

General Risk Factors	
Entity type designation in the US healthcare industry	Not a US healthcare entity
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)?	Yes
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)?	Yes
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)?	Yes
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)?	Yes

Does the organization use any part of the scoped systems, system components, or system services to sell goods and/or services?	Yes
Is the system(s) accessible from the Internet?	Yes
Number of interfaces to other systems	Greater than 75
Number of transactions per day	Greater than 85,000
Number of users of the system(s)	Greater than 5,500
Is the system(s) publicly positioned?	Yes
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?	Yes
Are hardware tokens used as an authentication method within the scoped environment?	Yes
Do any of the organization's personnel travel to locations the organization deems to be of significant risk?	Yes
Are wireless access points in place at any of the organization's in-scope facilities?	Yes

Compliance Factors (Optional)
PHIPA > Agent
PHIPA > Consumer Electronic Service Provider
PHIPA > Prescribed Organization
PHIPA > Researcher

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 Platforms

The following tables describes the platform that were 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

Customer Central (a.k.a. "Portal")	
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	2/29/22	Inheritance	(All in-scope platforms)	(All in-scope facilities)	(All assessment domains)

HITRUST

6. 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 PHIPA 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 PHIPA Compliance and is not a certification of PHIPA Compliance.

- This Insights 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 PHIPA compliance across the entirety of the Organization. Parties relying on this report should therefore evaluate the Scope in relation to the Organization's PHIPA 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 PHIPA compliance and were not designed to specifically detect all instances of PHIPA 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 PHIPA included in the Organization's HITRUST validated assessment and not in observance of any other criteria specific to PHIPA requirements.

- 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.

7. PHIPA Overview

Ontario's health sector is governed by the Personal Health Information Protection Act (PHIPA). PHIPA defines how personal health information (PHI) is handled by everyone in the healthcare system, while enabling appropriate access to data to support high-quality patient care and critical functions in the health system. Introduced in 2004, PHIPA built on leading principles for privacy protection in a health system context.

PHIPA has five stated purposes:

- To establish rules for the collection, use, and disclosure of PHI and to protect confidentiality of the information and privacy of individuals, while facilitating the effective provision of health care.
- To provide a right of access to individuals to their PHI (subject to limited exceptions).
- To provide a right of correction or amendment of PHI (subject to limited exceptions).
- To provide for independent review and resolution of complaints about PHI.
- To provide for effective remedies for contravention of the Act.

While PHIPA governs health information in Ontario, the federal Personal Information Protection and Electronic Documents Act (PIPEDA) applies to commercial activities involving the collection, use, or disclosure of personal information outside of Ontario. PIPEDA does not apply to personal information in provinces and territories that have "substantially similar" privacy legislation in place, and PHIPA has been deemed to be "substantially similar." PIPEDA may also apply if an organization collects, uses, or discloses information that is personal, but not health information, during commercial activities in Ontario (for example: collecting credit card information and a residential address to process sales that are not related to health data.)

Ontario's health system has changed in the years that have passed since the inception of PHIPA, thus PHIPA has been updated several times and was significantly amended on March 25, 2020. Like many other laws regulating personally identifiable health information, PHIPA contains significant privacy and security provisions (which are the main cornerstone of the HITRUST CSF).

The list below outlines in further detail the provisions/parts of PHIPA:

- **Part I** sets out the purposes of PHIPA, defines key terms, and explains the parties that PHIPA applies to.

- **Part II** outlines practices to protect personal health information practices mean the policies about when, how and the purposes for which the custodian/agent routinely collects, uses, modifies, discloses, retains or disposes of personal health information and the administrative, technical and physical safeguards and practices. Further defined Part II covers general provisions including electronic audit logs, accuracy, and security (including privacy breaches); record handling including location of records; accountability and openness including designated contact person, and responsibilities of both custodians and agents.

- **Part III** governs consent concerning personal health information: with limited exceptions, PHIPA requires health information custodians to obtain consent before they collect, use, or disclose personal health information.

- **Part IV** sets out general principles that apply to the collection, use and disclosure of personal health information such as minimum necessary information; indirect collection; and further details on collection, use, and disclosure, including those for fundraising or marketing purposes.

- **Part V** documents an individual's right to access and correction of their records of personal health information. Details on access/correction requests such as conditions for granting the rights of access, duty to correct, timeliness of response, format of records, fees, frivolous or vexatious requests, request refusal, and complaints to the Commissioner.

- **Part V.1,** Electronic Health Records (EHR), was added specifically to govern health information in digital or electronic form in the custody or control of a health information custodian/agents as part of the 2020 PHIPA amendments. Part V.1 governs which prescribed organizations can develop and maintain EHR electronic systems; requirements for electronic health record; EHR-related responsibilities of custodians; withholding or withdrawing consent; restrictions on collection use, disclosure by custodians; and details on privacy breaches involving electronic health records.

- **Part VI** establishes general provisions relating to the administration and enforcement of the legislation. Additionally, an appeal process is outlined so parties impacted by orders of the Commissioner may challenge those decisions in a court.

- **Part VII** contains several general provisions such as whistleblower protections, penalties for offences, and judicial proceedings for prosecuting offenses.

8. PHIPA Coverage and Reportability

A HITRUST validated assessment provides evidence that specific HITRUST CSF control requirements mapping to the portions of the Ontario Personal Health Information Protection Act (PHIPA) have been implemented, how well they have been implemented, and the nature and volume of identified gaps in implementation. The HITRUST CSF, the inherent mappings to PHIPA as a supported authoritative source, and HITRUST's comprehensive assurance program are important tools for organizations with PHIPA compliance obligations.

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

- HITRUST's approach to incorporating PHIPA into the HITRUST CSF
- The Organization's assessment type selection, HITRUST CSF version selection, and assessment tailoring
- Characteristics of the Organization (e.g., HIC, Agent, Researcher)

Approach to incorporating PHIPA into the HITRUST CSF

The HITRUST CSF intentionally does not provide full coverage of PHIPA, and intentionally does not contain mappings / cross-references to all text in the PHIPA law. Like many other authoritative sources, PHIPA contains several entries that are (a) necessary for its effective functioning as a law, but (b) are not directly actionable by organizations needing to achieve or evaluate compliance. These non-actionable entries are concentrated at the beginning (Part I) and ending (Part VII) of PHIPA but are found throughout all of PHIPA's parts.

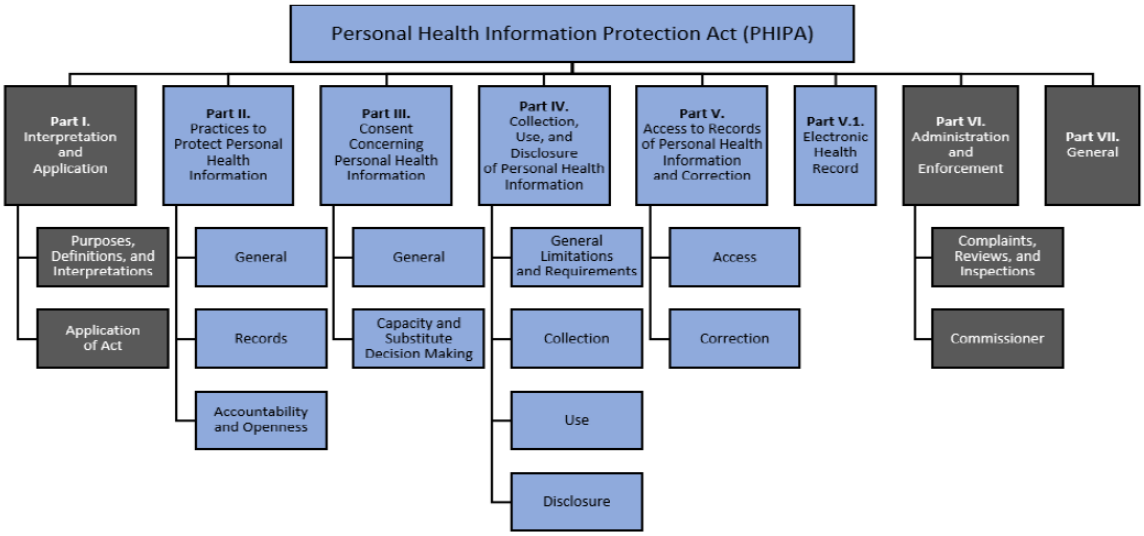
The non-actionable portions of PHIPA and can be categorized at a high level as follows:

Category of intentionally omitted PHIPA entry	Example PHIPA entry in this category
Stated purposes of the law itself	Part I, item 1: The purposes of this Act are, (a) to establish rules for the collection, use and disclosure of personal health information about individuals...
Definitions of key terms	Part I, item 2: In this Act, “Agency” means the corporation continued by section 3 of the Connecting Care Act, 2019...
Clarifications and interpretive guidance	Part II, item 15(3): A contact person is an agent of the health information custodian and is authorized on behalf of the custodian to,(a) facilitate the custodian's compliance with this Act...

Category of intentionally omitted PHIPA entry	Example PHIPA entry in this category
Assignment of oversight and enforcement responsibilities	Part V.1, item 55.11(4): The Ministry (a) shall provide administrative support for the advisory committee; (b) shall have custody and control of the records of the advisory committee for the purposes of the Freedom of Information and Protection of Privacy Act; and (c) is responsible for compliance with the Archives and Recordkeeping Act, 2006, in connection with records created by or supplied to the advisory committee. 2016, c. 6, Sched. 1, s. 1 (21).
Description of regulatory body and enforcement processes	Part VI, item 60(1): In conducting a review under section 57 or 58, the Commissioner may, without a warrant or court order, enter and inspect any premises in accordance with this section if…
Explanations of the applicability of PHIPA	Part I, item 7 (1): Except if this Act or its regulations specifically provide otherwise, this Act applies to…
Granting of authorities and abilities to entities within the Ontario healthcare system	• Part IV, item 37(1)(e): A health information custodian may use personal health information about an individual, (e) for educating agents to provide health care. • Part V.1, item 55.2(1): The prescribed organization has the power and the duty to develop and maintain the electronic health record in accordance with this Part and the regulations made under this Part.
Statements of individual rights	Part V.1, item 55.6(3): Subject to the limitations prescribed in the regulations, if any, an individual who has made a directive under subsection (1) may withdraw or modify the directive.

PHIPA entries identified by HITRUST as falling into one of the above omission categories—without also containing an actionable (i.e., implementable and verifiable) aspect—were intentionally not mapped against the HITRUST CSF due to their unactionable nature to organizations seeking to achieve or evaluate compliance with PHIPA. These PHIPA entries are also not reflected in the informative tables present throughout this PHIPA Insights Report.

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



Color	Meaning
Grey	Not mapped to the HITRUST CSF because not security or privacy related
Blue	Mapped to the HITRUST CSF

Impact of assessment preferences and tailoring on PHIPA 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 based on the unique risks and compliance needs of the Organization and on the HITRUST CSF version selected by the Organization (v11.2.0).

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 PHIPA; instead, only assessments utilizing version 11.2 and later can create PHIPA Insights Reports.

HITRUST

Organizational characteristics impacting PHIPA applicability and coverage

PHIPA contains requirements applicable only to certain types of organizations. For example, several PHIPA requirements apply only to Health Information Custodians, some apply only to the Prescribed Organization, while others apply only to Agents.

Specific to the HITRUST assessment scope, characteristics affecting the applicability of PHIPA requirements considered in the HITRUST r2 assessment underlying this PHIPA Insights Report are as follows:

Entity Type(s) per PHIPA (Agent, CESV, HIC, or PO)	Agent, Consumer electronic service provider (CESV), Prescribed organization (PO)
Researcher per PHIPA?	Yes
Health Data Institute per PHIPA?	No

HITRUST

Appendix A: PHIPA-relevant Observations

During the HITRUST assessment accompanying this PHIPA Insights Report, the policy, process, and/or 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 PHIPA compliance efforts, as each of these HITRUST CSF requirements map to one or more PHIPA requirements. The relying party should evaluate these items (and the associated risk treatment) in consultation with the Organization.

Part II

Mapped HITRUST CSF Requirement	Maturity level(s) scoring less than fully compliant	Reference	Management's stated corrective actions (unvalidated)
BUID: 19.13kPHIPAOrganizational.3 / CVID: 2735.0. The organization does not use or attempt to use information that has been de-identified to identify an individual unless specifically allowed by law to do so.	Procedure, Implemented	11.2(1)	No corrective action plans were communicated to HITRUST for this condition.
BUID: 19440.13kHIPAAOrganizational.12 / CVID: 1852.0. A business associate, or equivalent, only uses or discloses PHI as permitted or required by its business associate contract or other arrangement and does not use or disclose PHI in a manner that would violate requirements for the protection of such information, if done by the covered entity, or equivalent, except if such uses or disclosures are permitted by its contract or other arrangement.	Procedure, Implemented	17(1)(a), 17(1)(b), 17(1)(c)	No corrective action plans were communicated to HITRUST for this condition.

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 PHIPA considered in the underlying HITRUST CSF assessment, organized by PHIPA part.

This section also shows the HITRUST CSF requirements mapped by HITRUST to each considered PHIPA requirement. Note that many more mappings exist between PHIPA 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 PHIPA Coverage and Reportability section of this document.

In addition to PHIPA, 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.

The Organization believes certain of its products and/or services can assist its customers in meeting specific HITRUST requirement statements. The section below contains links to the HITRUST Products and Services Directory (PSD) where the Organization's customers can learn more.

Part II

HITRUST CSF Requirement	Policy Score	Procedure Score	Implemented Score
11.2(1) -Limits on use of de-identified information			
11.2(1) -Subject to subsection (2) and to any other exceptions that may be prescribed, no person shall use or attempt to use information that has been de-identified to identify an individual, either alone or with other information, unless this Act or another Act permits the information to be used to identify the individual.			

HITRUST CSF Requirement	Policy Score	Procedure Score	Implemented Score
BUID: 19.13kPHIPAOrganizational.3 / CVID: 2735.0. The organization does not use or attempt to use information that has been de-identified to identify an individual unless specifically allowed by law to do so.	Fully Compliant	Mostly Compliant	Somewhat Compliant

17(1) -Agents and information

17(1)(a) -(1) A health information custodian is responsible for personal health information in the custody or control of the health information custodian and may permit the custodian's agents to collect, use, disclose, retain or dispose of personal health information on the custodian's behalf only if,
(a) the custodian is permitted or required to collect, use, disclose, retain or dispose of the information, as the case may be;

BUID: 19440.13kHIPAAOrganizational.12 / CVID: 1852.0. A business associate, or equivalent, only uses or discloses PHI as permitted or required by its business associate contract or other arrangement and does not use or disclose PHI in a manner that would violate requirements for the protection of such information, if done by the covered entity, or equivalent, except if such uses or disclosures are permitted by its contract or other arrangement.	Fully Compliant	Mostly Compliant	Somewhat Compliant
BUID: 19441.13kHIPAAOrganizational.13 / CVID: 1853.1. The organization may disclose covered and/or confidential information to a service provider and may allow a service provider to receive, maintain, or transmit covered and/or confidential information on its behalf, if the organization obtains satisfactory, written assurance (e.g., a written contract, agreement or arrangement that satisfies the requirements of this control) that the service provider will appropriately safeguard the information.	Fully Compliant	Mostly Compliant	Somewhat Compliant

17(1)(b) -(1) A health information custodian is responsible for personal health information in the custody or control of the health information custodian and may permit the custodian's agents to collect, use, disclose, retain or dispose of personal health information on the custodian's behalf only if,
(b) the collection, use, disclosure, retention or disposal of the information, as the case may be, is necessary in the course of the agent's duties and is not contrary to this Act or another law; and

HITRUST CSF Requirement	Policy Score	Procedure Score	Implemented Score
BUID: 19441.13kHIPAAOrganizational.13 / CVID: 1853.1 The organization may disclose covered and/or confidential information to a service provider and may allow a service provider to receive, maintain, or transmit covered and/or confidential information on its behalf, if the organization obtains satisfactory, written assurance (e.g., a written contract, agreement or arrangement that satisfies the requirements of this control) that the service provider will appropriately safeguard the information.	Fully Compliant	Mostly Compliant	Somewhat Compliant
BUID: 19440.13kHIPAAOrganizational.12 / CVID: 1852.0 A business associate, or equivalent, only uses or discloses PHI as permitted or required by its business associate contract or other arrangement and does not use or disclose PHI in a manner that would violate requirements for the protection of such information, if done by the covered entity, or equivalent, except if such uses or disclosures are permitted by its contract or other arrangement.	Fully Compliant	Mostly Compliant	Somewhat 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 a harmonized information protection framework that incorporates and leverages the existing security requirements placed upon organizations, including international (e.g., GDPR, ISO), federal (e.g., FFIEC, HIPAA), state / province (e.g., PHIPA, CCPA), third party (e.g., PCI, COBIT), and other government agencies (e.g., NIST, FTC, 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.

For more information about HITRUST, the HITRUST CSF and other HITRUST offerings and programs, visit https://hitrustalliance.net.