Privacy Impact Assessment for Google Cloud

Conducted for Google

April 2023

120 Carlton Street, Suite 416
Toronto, ON M5A 4K2
t. 416.642.2081
e. info@mdahealth.ca

Contents

Executive Summary

Project Background

Several privacy laws and regulations in Canada protect healthcare data. In addition to federal laws such as PIPEDA, provinces maintain provincial health privacy laws such as the Personal Health Information Protection Act, 2004 (PHIPA) in Ontario. To support Google Cloud's Canadian healthcare and public sector customers who use our services to process healthcare data, we engaged an independent third party to conduct a Privacy Impact Assessment (PIA) of Google Cloud services available in Canada. While customers are responsible for their PIAs, they can use this assessment to ease the process, cost, and resources of conducting assessments. The Google Cloud PIA addresses privacy requirements for our Canadian-based healthcare customers who may be subject to PHIPA and PIPEDA when using Google Cloud services.

Summary of Findings and Recommendations

In selling Google Cloud services for Ontario healthcare, Google Cloud acts as a service provider to customers who have privacy obligations. Google Cloud capabilities enable those customers to meet their own requirements under PHIPA. In meeting their obligations under PHIPA, Google states: "Customers can rely on Google and their tools for supporting them in their compliance journey for their obligations under the law. Google complies with its own obligations under the law, including privacy laws."

Customers of Google Cloud, whether healthcare organisations or organisations developing products and services on Google Cloud services to resell to healthcare organisations (henceforth referred to as an End Product Provider or EPP), are responsible for their own privacy obligations and should follow the appropriate guidance in creating products and services on Google Cloud services.

1 Introduction

This privacy impact assessment (PIA) has been prepared for Google to provide a privacy assessment of the individual services contained in Google Cloud in context of Ontario's *Personal Health Information Protection Act* (PHIPA) and Canada's *Personal Information Protection and Electronic Documents Act* (PIPEDA).

A complete list of the technical components considered as part of Google Cloud is in Appendix A with additional inline privacy commentary.

This document is intended for Ontario healthcare organisations subject to PHIPA and / or organisations building healthcare products and services for the Ontario healthcare sector on Google Cloud to understand Google's roles and responsibilities under PHIPA and also for private sector organisations in Canada subject to the PIPEDA federal privacy law .

The PIA:

- Describes Google Cloud privacy practices in the context of the technical services available in Canada listed in Appendix A;
- Sets out Google role as a service provider to custodians or other customers and subsequent responsibilities in respect of Ontario's PHIPA and Canada's PIPEDA;
- Identifies (if any) outstanding areas of risk for Google Cloud; and
- Provides recommendations to address outstanding risks (if any) for Google Cloud.

The PIA does not:

- Address physical, technical or security safeguards, e.g., encryption;
- Consider other federal or provincial obligations (legislative or otherwise) for research
- Consider the provenance of PHI or PI that may be contained or moved through Google Cloud; or,
- Consider any other Google or Google branded products, including Google Workspace, Gmail, Drive, etc.

2 Overview of Google Cloud

NB: For the sake of this document, the term "end product" is used to denote the applications and services that utilise Google Cloud's capabilities.

In the pre-cloud IT model, organisations maintained full responsibility for their environment managing physical infrastructure, networking, security controls and applications. Google Cloud is representative of the cloud-based IT model. For the purposes of this assessment, in the cloud-based IT model for healthcare organisations, the many obligations of managing the IT environment are shared between the provider (Google), the EPP (where applicable), and the healthcare organisational customer.

Google's public documentation refers to this as a 'shared fate model'. Google Cloud developed the shared fate model to start addressing their perspective that the shared responsibility model is

incomplete. Rather, Google believes the notion of shared fate builds on the shared responsibility model because it views the relationship between cloud provider and customer as an ongoing partnership to improve security. In the previous shared responsibility model, both Google Cloud and the customer have responsibilities based on the consumption model (Iaas, PaaS, or SaaS) chosen. Examples of the responsibilities that Google Cloud can provide in such a model include physical security to underlying infrastructure, and providing administrative consoles for end products and organisational customers to identify, establish and manage their privacy obligations. By contrast, a key component of shared fate involves providing resources to help customers get started, including security foundations, secure blueprints, architecture framework best practices, and landing zone navigation guides.

Google Cloud includes 100+ products and services across 19 categories that range from developer consoles, to services like compute, database and machine learning. These services can be used in a broad range of ways by Google Cloud customers, to deliver healthcare-centric solutions.

Google Cloud offers inbuilt physical, technical, and administrative controls that can be used to safeguard customer data (PHI/PII). Customers can exert further control on their data through capabilities such as customer supplied encryption keys (CSEK), Cloud External Key Manager (Cloud EKM), Cloud Hardware Security Module (Cloud HSM), Key Access Justification (KAJ) and Assured Workloads. Google Cloud services are data agnostic; not built specifically with the consideration of personal health information (PHI, as defined under PHIPA) or personal information (PI, as defined under PIPEDA).[1] However, Google Cloud offers some services that are specifically built with PHI considerations (e.g., a healthcare application programming interface (API) built for the Fast Healthcare Interoperability Resources (FIHR), Healthcare Natural Language API). When used for the collection, use and disclosure of PHI consistent with Google's Shared Fate Model, these services must be configured by Google Cloud customers in accordance with both Google's published best practice configuration guidance and with consideration of the appropriate privacy obligations that may apply to the EPP or healthcare organisational customer.

2.1 Roles & Responsibilities

As stated earlier, PHIPA sets out obligations for named entities handling PHI in Ontario while PIPEDA sets out private sector obligations handling PI across Canada. The following table provides a summary of organisational parties along with the roles and responsibilities (if any) they have in the use of Google Cloud.

[1] See PHIPA s.4 at https://www.canlii.org/en/on/laws/stat/so-2004-c-3-sch-a/latest/so-2004-c-3-sch-a.html#sec4_smooth and PIPEDA s.2 at https://laws-lois.justice.gc.ca/PDF/P-8.6.pdf.

Organisation	Role	Commentary
Google	Provider of cloud based services	Under PHIPA, in selling Google Cloud in Ontario Google is an Electronic Service Provider (ESP).[2] Under PIPEDA, in selling Google Cloud in Ontario, Google does not *by design* directly handle PI except where described in Section 3 of this assessment.
End Product Providers (EPP)	Provider of healthcare solutions built on Google Cloud.	Under PHIPA, in building solutions on Google Cloud to sell to healthcare organisations, EPPs are likely to be ESPs, HINPs, or agents. In Ontario, PIPEDA may or may not apply to these organisations depending on the nature of the solutions provided. This PIA can be used as an input for these organisations but does not assess their privacy obligations, nor fulfil the obligation to undertake a solution PIA.
Healthcare Organisations	Customer of EPP healthcare solutions; possibly a direct customer of Google Cloud.	Under PHIPA, in purchasing and using healthcare solutions built on Google Cloud to support the provision of healthcare services that involve the processing of PHI, these organisations are HICs. In the event of developing in-house solutions built on Google Cloud or leading the procurement of an EPP hosted in Google Cloud, these healthcare organisations could also function as an agent, ESP and/ or HINP for other HICs who contract with them to use the same solution. In any of these cases, this PIA can be used as an input for these organisations but does not assess their obligations in the use of these solutions. In Ontario, PIPEDA would not apply to these organisations.
Patient / Individual	Data subject (including guardian or substitute decision-maker)	The individual person whose PHI / PI is collected, used and disclosed in a given healthcare solution. The privacy rights of individuals spelled out under PHIPA and PIPEDA are considered in this document only insofar as Google's obligations are concerned.

[2] See Google Cloud data processing addendum: https://cloud.google.com/terms/data-processing-addendum.

3 Privacy Commentary

In keeping with Google's shared fate model, customers of Google Cloud should be aware of their own obligations in using cloud services. Google provides guidance, best practices and additional documentation along with this PIA to highlight the key privacy considerations that may impact Ontario healthcare organisations. Google Cloud customers can leverage Google's certifications and services to help fulfil their own obligations, noting that these may be similar to but not encompassing other provincial privacy and health privacy laws, which are not specifically assessed in this document.

This section of the PIA considers privacy requirements stemming from privacy legislation and relevant standards along with the privacy roles of Google and its Google Cloud customers and Google's corresponding roles outlined in Section 2.

3.1 Regionalization

Given the shared fate model, organisations can use the available controls to ensure PI or PHI is only stored or processed in the defined regions (provincially or nationally). Where PI or PHI moves outside of these regions, it is the responsibility of organisations to ensure their obligations are met. See Appendix A for a detailed list of Google Cloud services including regions where they are available.

3.2 Authority for Collection, Use, and Disclosure

In selling Google Cloud, Google is not required to establish authority for collection, use and disclosure. Healthcare organisations who purchase services, either directly or through an EPP, are required to demonstrate the necessary authority. Google Cloud does not intentionally collect, use or disclose PHI or PI for the purposes of providing Google Cloud services. Specific circumstances are highlighted in Google's contractual commitments, e.g. section 7 titled "Data Security" in Google's CDPA.

Google Administrators may access and use data that may include PHI/PI under limited and specific circumstances; e.g. as part of delivering a contracted service such as to investigate a support ticket lodged by the customer,[3] or disclose under a legal subpoena by a government agency. Google has published a whitepaper outlining the policy, practice, and process through which government agencies may request access to customer data in Google Cloud.

Google logs each occurrence of access, use or disclosure together with a valid business justification and these logs are available in near real-time through the Access Transparency feature and Access Approval

[3] See https://cloud.google.com/cloud-provider-access-management/access-transparency/docs/privileged-access for additional details.

process in Google Cloud[4], which requires customer approval of any Google employee access for support requests. An example provided by Google:

> *Google receives abuse reports and legal removal requests related to the use/misuse of our products and services. When we receive these complaints, we will investigate and take action if appropriate. In general, these complaints consist of data from a reporter and an identification of content or activity that they consider to be abusive.*[5]

Google notes that it might itself use patterns of activity consistent with known or suspected abusive behaviour to trigger action to limit abuse.

Google Cloud customer information may be obtained by third parties through legal processes, including search warrants, court orders, subpoenas, legal or regulatory requirements, or through user consent. Upon receipt of a request for information disclosure, Google's Legal team reviews the request for compliance with applicable law, and in the current public online terms indicate Google will use commercially reasonable efforts to try to "*object to, or limit or modify, any Legal Process that the Recipient reasonably determines is overboard, disproportionate, incompatible with applicable law, or otherwise unlawful.*" If the request is legally valid, it is Google's policy to notify the individual user or organisation whose information is being requested except in an emergency or where prohibited by law.

3.3 Governance and Accountability

Google has numerous certifications for Google Cloud incorporating multiple controls to ensure all personnel are aware of their roles and responsibilities, including maintaining awareness and compliance with established policies and procedures and applicable legal, statutory or regulatory compliance obligations.[6] Google maintains a public website that details all current compliance, regulatory, and privacy standards with which Google either complies or aligns.

3.3.1 Agreements

Google's data processing terms related to the handling of customer data are detailed in an online set of terms. Additional information about the provision of Google Cloud services to healthcare organisations and /or EPPs are detailed in an online whitepaper. In some limited and specific circumstances Google may be considered an ESP (see table above).

---

[4] Google reports: "... access rights are based on a Google employee's job function and role—using the concepts of least-privilege and need-to-know—commensurate with the employee's defined responsibilities. Google employees are only granted a limited set of default permissions to access company resources. Google requires the use of a unique user ID for each employee. This account is used to identify each person's activity on Google's network, including any access to employee or customer data." See: https://cloud.google.com/logging/docs/audit/access-transparency-overview for details on the transparency report.

[5] See: Reporting Abuse Incidents - Google Workspace Admin Help for details.

[6] Google reports controls mapped to: CSA Guidance v3.0: Domain 2, AICPA/SOC 2 Controls: CC3.2 as well as numerous ISO standards and NIST. Publicly available compliance reports: https://cloud.google.com/security/compliance/compliance-reports-manager.

3.3.2 Privacy Training and Awareness

Google has established privacy and information security training programs and requires personnel to complete this training annually. All Google employees undergo security and privacy training as part of the orientation process, and they receive ongoing security and privacy training throughout their Google careers. During orientation, new employees are also required to agree to Google's Code of Conduct, which highlights Google's commitment to keep customer information safe and secure. Role-based job training is provided, e.g. the Google Cloud information security team instructs new engineers on topics like secure coding practices, product design and automated vulnerability testing tools. Engineers also attend technical presentations on security-related topics and receive a security newsletter that covers new threats, attack patterns, mitigation techniques and more.[7]

3.4 Consent

In selling Google Cloud, Google provides the underlying platform and services and does not directly obtain consent from data subjects. EPPs are responsible for obtaining any consent required for the product they design and operate on top of Google Cloud, and healthcare organisations using these products are required to obtain and manage consent directly as a consumer of such EPP and / or for their own solutions developed and/or operated on Google Cloud.

Google offers an API, included in the Healthcare API, known as the consent management service (Consent Management API). This service offers tools for organisations to establish consent policies, store artefacts, and track the type of policies in place.[8] The Consent Management API stores the consent information received from data subjects, keeps track of what data is permitted for each use case, and helps applications utilise data only as directed by data subjects.[9] Aside from the technical capabilities of this service, Google has an opportunity to provide guidance to customers on how to configure consent to ensure compliance. Today, healthcare organisations and EPPs can configure this capability to address consent management requirements on their own.

[7] FedRAMP SSP v8.9. See Appendix for a complete list of audits. See https://cloud.google.com/security/overview/whitepaper#security_training_for_all_employees for additional details on employee training, and https://cloud.google.com/privacy for additional information.
[8] Note: user data mappings are stored within the Consent Management API while the managed resources are stored outside the Consent Management API.
[9] Relevant links to explain how the Consent Management API can be used: 1) Consent and privacy overview, 2) Prescriptive guidance on creating and managing consent stores, 3) Prescriptive guidance on configuring consent policies using attributes, 4) Prescriptive guidance on creating and updating user consents, 5) Prescriptive guidance on registering user data, 6) Prescriptive guidance on making access determinations.

3.5 Privacy Standards for Information Management

3.5.1 Limiting Collection, Use, and Disclosure

In selling Google Cloud, Google provides the underlying platform and services and is not directly responsible for setting limitations on collection, use and disclosure. Customers using Google Cloud, including healthcare organisations and EPPs are responsible for controlling any such limitations.

In using Google Cloud, healthcare organisations and EPPs must explicitly assign identities (users, groups, and service accounts) permissions to access or modify resources. These permissions can be set at multiple levels within the Resource Manager hierarchy. Only internal/external identities approved by the customer will have access to potential PHI data using the least privilege access principle. The Cloud Data Loss Prevention (DLP) service can be employed to de-identify data while maintaining usability for analytics.

3.5.2 Retention and Disposal

In selling Google Cloud, Google provides the underlying platform and services. Customers of Google Cloud maintain full control and accountability for backup, retention, and disposal of their data. Google is not directly responsible for retention and disposal practices, which remain the responsibility of the customer. In its data processing terms, Google commits, "*.. if customers delete their data, we commit to deleting it from our systems within 180 days.*"

3.6 Privacy Operations

3.6.1 Requests for Access and Correction

Under PIPEDA and PHIPA, data subjects have a right of access and correction to their data. In selling Google Cloud, Google is not responsible for processing such requests. However,

> *"... if Google's Cloud Data Protection Team receives a request from a data subject that relates to Customer Personal Data and identifies Customer, Google will: (a) advise the data subject to submit their request to Customer; (b) promptly notify Customer; and (c) not otherwise respond to that data subject's request without authorization from Customer. Customers will be responsible for responding to any such request including, where necessary, by using the functionality of the Services."*[10]

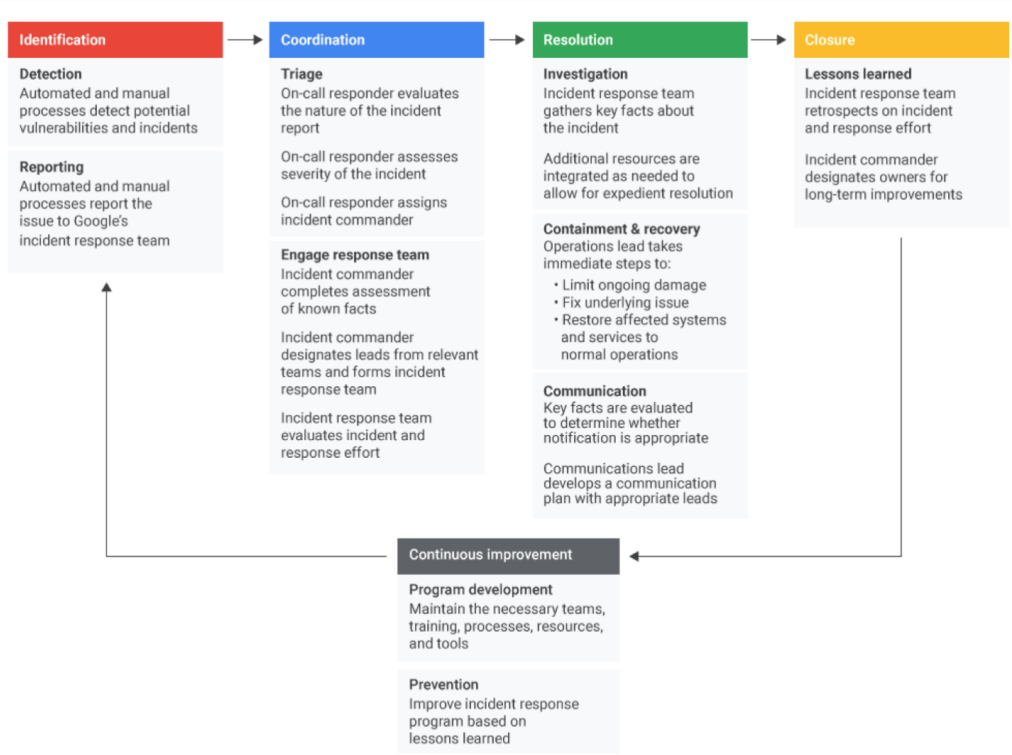
Healthcare organisations and EPPs should have processes in place to manage these notifications and requests as appropriate.

[10] Section 9.2 in the CDPA

3.6.2 Privacy Breach Management

HICs are responsible for managing privacy breaches. Google Cloud has built a program to help customers with data incidents, with more information available here, and has made commitments to notify customers promptly after becoming aware of a breach.[11]

It provides details on the Google Cloud data incident response plan, including the following workflow:



As part of the remediation stage, Google commits to:

> *…notifying customers when incidents impact their data. Key facts are evaluated throughout the incident to determine whether the incident affected customers' data. If notifying customers is appropriate, the incident commander initiates the notification process. The communications lead develops a communication plan with input from the product and legal leads, informs those affected, and supports customer requests after notification with the help of our support team.*
>
> *Google strives to provide prompt, clear, and accurate notifications containing the known details of the data incident, steps Google has taken to mitigate the potential risks, and actions Google recommends customers take to address the incident. We do our best to provide a clear picture of the incident so that customers can assess and fulfil their own notification obligations.*[12]

[11] Section 7.3 in the CDPA. See also:
[12] Google, Google Cloud Data Incident Response Plan: https://cloud.google.com/docs/security/incident-response.

Timelines, types and details of the notifications are not prescribed.

3.7 Assurance and Risk Management

Google has created a number of compliance guides, white papers, blog posts, admin help spaces and related documents to reinforce the shared fate model for compliance. A number of these resources address privacy risk outside of a specific risk assessment. See Appendix B for a list of this documentation, which demonstrates Google's understanding and ability to meet their privacy obligations and can be used to help customers understand what compliance activities they are responsible for.

To start, Google Cloud customers own their own data. Google states:

> *…implements stringent security measures to safeguard your customer data and provide you with tools and features to control it on your terms. We similarly secure any service data generated through providing the services; service data itself is critical to help ensure security and availability.*[13]

Google Cloud customers may conduct an audit to verify Google's compliance with its obligations under the Cloud Data Processing Addendum (CDPA) by reviewing the Security Documentation (which reflects the outcome of audits conducted by Google's Third-Party Auditor).

Similarly in building solutions on Google Cloud to sell to healthcare organisations, EPPs are likely to themselves be ESPs, HINPs, or agents. In this case, these Google Cloud customers who are EPPs are likely to have additional requirements from PHIPA for specific role-based obligations. In the event of developing its own in-house solutions built on Google Cloud, healthcare organisations themselves could function as an agent, ESP and/ or HINP where the organisation provides the EPP to other custodians. In these cases, customers may ask Google for specific assistance in, for example, conducting and providing the results of risk assessments.

3.7.1 Logging

Cloud Logging is a fully managed Google Cloud service to store, search, analyse, monitor, and alert on logging data and events. Data can be collected from over 150 common application components and cloud systems. The service includes storage for logs, a user interface and an API. Logging functionality is dependent on the specific implementation of Google Cloud services by the EPP and / or healthcare organisation. Google Cloud customers can take advantage of Google tools for HICs to meet the PHIPA 'Electronic Audit Log' requirements as well as other obligations.[14]

[13] Google Cloud, Expanding our privacy commitments to our customers: https://cloud.google.com › blog › products › identity-security › expanding-our-privacy-commitments-to-customers.

[14] Google Cloud resources to deploy logging capabilities: Understanding audit logs - talks about specific details that are captured in audit logs and aligns with PHIPA 10.1(4). Outlining Google Cloud logging and configuration: Cloud Audit Logs Overview,Configure data access audit logs, Cloud Audit Logs Overview, Best practices for Cloud Audit Logs, Monitor your logs.

Access to customer data is logged and intelligent threat detection systems conduct real-time audits, alerting staff when log entries match threat indicators. Internal security teams evaluate alerts and logs to identify and investigate anomalous activities, limiting the scope and impact of any incident. Incident response is discussed further in the data incident response process whitepaper.

Appendix A: Catalogue of Google Cloud Available Products

With Google Cloud, Google offers “building blocks”. Continuing from above, the term “end product” refers to a set of applications and services that an EPP or healthcare organisation builds on Google Cloud. Any information transfer or compute resources that handle PHI or PI are assumed to be configured to reside solely in Google Cloud regions within Canadian jurisdiction unless noted otherwise herein (See ‘Regionalization’ in Section 3 for details). Toronto region launched in Sept 2021 with a subset of Google Cloud services. Services not available in Toronto will be noted below.

A full list of currently available services at present time available in Canadian regions (Montreal - northamerica-northeast1 and Toronto - northamerica-northeast2) can be found via the following link: https://cloud.google.com/about/locations.

Container Compute

- Google Kubernetes Engine (GKE) - Managed environment for running containerized apps.
- Deep Learning Containers - Containers with data science frameworks, libraries, and tools pre-installed.

Privacy Impact:
End Products / Healthcare Organisations utilising Google Cloud’s Container capabilities, which process data subject to privacy obligations, should be configured in accordance with Google’s best practices and in considerations of any additional obligations under PHIPA.

Regional Restrictions:
None

Developer Tools

- Cloud SDK - Command-line tools and libraries for Google Cloud
- Artifact Registry - Store, manage, and secure container images and language packages.
- Cloud Build - Continuous integration and continuous delivery platform.
- Cloud Source Repositories - Private Git repository to store, manage, and track code.
- Cloud Scheduler - Cron job scheduler for task automation and management.
- Cloud Tasks - Task management service for asynchronous task execution.
- Tools for Visual Studio - Tools to enable development in Visual Studio on Google Cloud.
- Tools for PowerShell - Full cloud control from Windows PowerShell.

Privacy Impact:
Developer tools that require or grant access to developer/operations staff to production data subject to privacy obligations should be configured in accordance with Google’s best practices for secure and auditable data processing and in consideration of any additional obligations under PHIPA. Specifically command-line tools: **Cloud SDK** and **Tools for Powershell**.

Regional restrictions:
Available only in Montreal region

- Cloud Scheduler
- Cloud Tasks

○ Migration

- BigQuery Data Transfer Service - Data import service for scheduling and moving data into BigQuery.
- Cloud Foundation Toolkit - Reference templates for Deployment Manager and Terraform.
- Storage Transfer Service - Data transfers from online and on-premises sources to Cloud Storage.
- Migrate for Anthos - Components for migrating VMs into system containers on GKE.
- Migrate for Compute Engine - Components for migrating VMs and physical servers to Compute Engine.
- Transfer Appliance - Storage server for moving large volumes of data to Google Cloud.

Privacy Impact:
End Products / Healthcare Organisations that utilise migration tools to import data, subject to privacy obligations into Google Cloud Services (**BigQuery Data Transfer**, **Storage Transfer Service**, and **Transfer Appliance**) should include verification that migration targets are properly configured per Google's best practices and are located in Canadian Google Cloud regions.

Regional Restrictions:
None

○ Security and Identity

- Access Transparency - Cloud provider visibility through near real-time logs.
- Binary Authorization - Deploy only trusted containers on Kubernetes Engine.
- Cloud Asset Inventory - View, monitor, and analyse Google Cloud and Anthos assets across projects and services.
- Cloud Audit Logs - Gain visibility into who did what, when, and where for all user activity on Google Cloud.
- Cloud Data Loss Prevention - Sensitive data inspection, classification, and redaction platform.
- Cloud External Key Manager - Encrypt data using a third-party key management system.
- Cloud HSM - Crypto key protection with a managed hardware security service.
- Cloud Key Management Service - KMS for creating, importing, and managing cryptographic keys.
- Security Command Center – Platform for defending against threats to your Google Cloud assets.
- Shielded VMs - –Virtual machines hardened with security controls and defences.
- VPC Service Controls - Protect sensitive data in Google Cloud services using security perimeters.
- Chronicle - Extract signals from your security telemetry to end threats instantly.
- Secret Manager - Store API keys, passwords, certificates, and other sensitive data.

Privacy Impact:
Google Cloud offers a rich set of Security and Identity services which End Products can use for authorization, authentication, and audit logging. End Product / Healthcare Organisations use of **Cloud Audit Logs** should follow Google's best practices for securing log information to appropriate parties and in considerations of any additional obligations under PHIPA. Google Cloud's Cloud Data Loss Prevention Service (DLP) provides a means to perform classification and de-identification of PHI and PI and End Product *could* be used to comply with the subject regulatory environment. Details regarding *how* End Products could utilise DLP for this purpose is offered by Google Cloud's best practices and is beyond the scope of this document. Access Transparency is also available in Canada.[15]

○ API Management

- Apigee API Platform - API management, development, and security platform.
- API Analytics - Dashboards, custom repos, and metrics for API performance.
- API Monetization - Revenue stream and business model creation from APIs.
- Apigee Hybrid - Deployment option for managing APIs on-premises or in the cloud.
- Apigee Sense - Intelligent behaviour detection to protect APIs.
- Cloud Endpoints - Deployment and development management for APIs on Google Cloud.
- Apigee Developer Portal - Self-service and custom developer portal creation.

Privacy Impact:
EPPs / Healthcare Organisations which utilise Google Cloud's API Management capabilities should follow Google's best practices for API security, access control, and logging.

○ Identity & Access

- Cloud Identity and Access Management - Permissions management system for Google Cloud resources.
- Cloud Identity – Unified platform for IT admins to manage user devices and apps.
- Identity-Aware Proxy - Use identity and context to guard access to your applications and VMs.
- Context-aware access - Manage access to apps and infrastructure based on a user's identity and context.
- Identity Platform - Add Google-grade identity and access management to your apps.
- Managed Service for Microsoft Active Directory - Hardened service running Microsoft Active Directory (AD).
- Policy Intelligence – Smart access control for your Google Cloud resources.
- Resource Manager - Hierarchical management for organising resources on Google Cloud.
- Titan Security Key - Two-factor authentication device for user account protection.

Privacy Impact:
End Products / Healthcare Organisations utilising these services should follow Google's best practices for identity management, policy and lifecycle for access to PHI and PI, regional residency of services and in

[15] https://cloud.google.com/cloud-provider-access-management/access-transparency/docs/supported-services.

considerations of any additional obligations under PHIPA..

Regional Restrictions:
None

○ User Protection Services

- reCAPTCHA Enterprise - Help protect your website from fraudulent activity, spam, and abuse.

Privacy Impact:
None

Regional Restrictions:
N/A

○ Serverless Computing

- Cloud Run - Compute platform for running and scaling stateless containers.
- App Engine - Serverless application platform for apps and back ends.
- Cloud Functions – Platform for creating functions that respond to cloud events.
- Knative - Components to create Kubernetes-native cloud-based software.

Privacy Impact:
EPPs / Healthcare Organisations utilising Google Cloud's Serverless compute capabilities which process PHI and PI should be configured in accordance with Google's best practices for secure and auditable data processing.

Regional Restrictions:

Services available only in Montreal region

- App Engine

○ Management Tools

- Private Catalog - Service catalogue for admins managing internal enterprise solutions.
- Cloud Deployment Manager - Service for creating and managing Google Cloud resources.
- Cloud Console - Web-based interface for managing and monitoring cloud apps.
- Cloud Shell - Interactive shell environment with a built-in command line.
- Cloud Mobile App - App to manage Google Cloud services from your mobile device.
- Cost Management - Tools for monitoring, controlling, and optimising your costs.

Privacy Impact:
EPPs / Healthcare Organisations utilising Google Cloud's Management tools should be configured and operated in accordance with Google's best practices for secure and auditable data processing and in consideration of any additional obligations under PHIPA.

Regional restrictions:
None

○ Compute

- Compute Engine - Virtual machines running in Google's data centre.
- Bare Metal - Infrastructure to run specialised workloads on Google Cloud.
- Cloud GPUs - GPUs for ML, scientific computing, and 3D visualisation.
- Migrate for Compute Engine - Server and virtual machine migration to Compute Engine.
- Preemptible VMs - Compute instances for batch jobs and fault-tolerant workloads.
- Recommender - Proactive, easily actionable recommendations to keep your cloud optimised.
- Shielded VMs - Reinforced visual machines on Google Cloud.
- Sole-tenant nodes - Dedicated hardware for compliance, licensing, and management.
- VMware Engine - Migrate and run your VMware workloads natively on Google Cloud.

Privacy Impact:
EPPs / Healthcare Organisations utilising Google Cloud's Serverless compute capabilities which process data subject to privacy obligations should be configured in accordance with Google's best practices for secure and auditable data processing.

Regional Restrictions:
None

○ Storage

- Cloud Storage - Object storage that's secure, durable, and scalable.
- Persistent Disk - Block storage for virtual machine instances running on Google Cloud.
- Filestore - NFS for apps and data that require le system capabilities.
- Local SSD - Local solid-state drive storage for virtual machine instances.

Privacy Impact:
EPPs / Healthcare Organisations utilising Google Cloud's capabilities which process data subject to privacy obligations should be configured in accordance with Google's best practices for secure and auditable data processing and in consideration of any additional obligations under PHIPA.

Regional Restrictions:
None

○ Databases

- Cloud Bigtable - NoSQL wide-column database for storing big data with low latency.
- Memorystore - In-memory data store service for Redis for fast data processing.
- Cloud SQL - Relational database services for MySQL, PostgreSQL, and SQL Server.

Privacy Impact:

Healthcare organisations and EPPs utilising Google Cloud's database services capabilities which process data subject to privacy obligations should be configured in accordance with Google's best practices for secure and auditable data processing.

Regional Restrictions:
None

○ Operations

- Cloud Logging - Logging for applications on Google Cloud and AWS.
- Cloud Monitoring - Monitoring for applications on Google Cloud and AWS.
- Kubernetes Engine Monitoring - Aggregates for logs, events, and metrics from your environment.
- Cloud Trace - Tracing system collecting latency data from applications.
- Cloud Audit Logs - Tool for tracking admin activity and maintaining audit trails.

Privacy Impact:
EPPs / Healthcare Organisations who utilise Google Cloud's logging services should insure services configurations/operations are configured in accordance with Google's best practices for secure and auditable data processing and in consideration of any additional obligations under PHIPA.

Regional Restrictions:
None

○ Networking

- Cloud Armor - Security policies and defence against web and DDoS attacks.
- Cloud CDN - Content delivery network for serving web and video content.
- Cloud DNS - Domain name system for reliable and low-latency name lookups.
- Cloud Load Balancing - Service for distributing trac across applications and regions.
- Cloud NAT - NAT service for giving private instances internet access.
- Hybrid Connectivity - Connectivity options for VPN, peering, and enterprise needs.
- Network Intelligence Center - Network monitoring, verification, and optimization platform.
- Network Telemetry - VPC flow logs for network monitoring, forensics, and security.
- Virtual Private Cloud (VPC) - Virtual network for Google Cloud resources and cloud-based services.

Privacy Impact:
EPPs / Healthcare Organisations utilising Google Cloud's Networking services which transit data subject to privacy obligations should be configured in accordance with Google's best practices for secure and auditable data processing.

Regional Restrictions:
None

○ Data Analytics

- BigQuery - Data warehouse for business agility and insights.
- Looker - Platform for BI, data applications, and embedded analytics.
- Cloud Composer - Work ow orchestration service built on Apache Airflow.
- Dataflow - Streaming analytics for stream and batch processing.
- Cloud Data Fusion - Data integration for building and managing data pipelines.
- Dataprep - Service to prepare data for analysis and machine learning.
- Dataproc - Service for running Apache Spark and Apache Hadoop clusters.
- Google Data Studio - Interactive data suite for dashboarding, reporting, and analytics.
- Pub/Sub - Messaging service for event ingestion and delivery.
- Data Catalog - Metadata solution for exploring and managing data.

Privacy Impact:
EPPs / Healthcare Organisations utilising Google Cloud's data analytics services could include PHI or PI, and should be configured in accordance with Google's best practices for secure and auditable data processing, the use of de-identification services where appropriate, and in considerations of any additional obligations under PHIPA.

Regional Restrictions:

Services available only in Montreal region:

- Cloud Composer

○ AI and Machine Learning

- AutoML - Custom machine learning model training and development.
- Vision AI - Custom and pre-trained models to detect emotion, text, more.
- Video AI - Video classification and recognition using machine learning.
- Cloud Natural Language - Sentiment analysis and classification of unstructured text.
- Cloud Translation - Language detection, translation, and glossary support.
- Media Translation (beta) - Add dynamic audio translation directly to your content and applications.
- Text-to-Speech - Speech synthesis in 180+ voices and 30+ languages.
- Speech-to-Text - Speech recognition and transcription supporting 120 languages.
- Dialog ow - Conversation applications and systems development suite.
- Cloud Inference API (alpha) - Quickly run large-scale correlations over typed time-series datasets.
- Document AI - Automate document data capture at scale.

Privacy Impact:
EPPs / Healthcare Organisations utilising Google Cloud's AI and Machine learning capabilities which process data subject to privacy obligations should be configured in accordance with Google's best practices for secure and auditable data processing, the use of de-identification services where

appropriate, and in considerations of any additional obligations under PHIPA.

Regional Restrictions:
Services not available in Canadian Regions:
- Vision AI
- Video AI
- Cloud Natural Language
- AutoML Translation

Services available only in Montreal region:
- Document AI

○ Vertex AI and Accelerators

Vertex AI Managed Notebooks
- Vertex AI - Platform for training, hosting, and managing ML models.
- Vertex AI Deep Learning VM Image - Pre Configured VMs for deep learning applications.
- Vertex AI Managed Notebooks - An enterprise notebook service to get projects up and running in minutes.
- Cloud TPU - Tensor processing units for machine learning applications.

Privacy Impact:
EPPs / Healthcare Organisations utilising Google Cloud's Vertex AI and Accelerators which process data subject to privacy obligations should be configured in accordance with Google's best practices for secure and auditable data processing, the use of de-identification services where appropriate and in considerations of any additional obligations under PHIPA.

Regional Restrictions:
- Of the 19 Vertex AI features 14 are available in the Toronto and Montreal Google Cloud regions.[16]

○

○ Healthcare Industry Focused Google Cloud Services

- Healthcare API - Solution to bridge existing care systems and apps on Google Cloud.
  - FHIR API & Store
  - DICOM API & Store
  - HL7v2 API & Store
- Healthcare NLP (Natural Language Processing) API - ML to derive insights from medical texts.
- Healthcare API De-Identification (FHIR & DICOM) - Removing identifying information from data in FHIR & DICOM
- Apigee Healthcare APIx - Easily build FHIR API based digital services.

[16] See this page for up-to-date information on Vertex AI features available regionally: https://cloud.google.com/vertex-ai/docs/general/locations.

- Cloud Life Sciences API - suite of services and tools for managing, processing and transforming life sciences data.

Privacy Impact:
EPPs / Healthcare Organisations utilising Google Cloud's Healthcare API and related services should be configured in accordance with Google's best practices for secure and auditable data processing where appropriate and in consideration of any additional obligations under PHIPA.

Healthcare API platform implements a Consent Management API which allows for the creation, management, and instrumentation of one or more consent models that End Product can use to manage consent resources. Healthcare API platform implements a De-Identification service which can be utilised to de-identify data created or imported into the Healthcare API store by the End Product. Google Cloud's Healthcare API provides a range of healthcare industry standard capabilities (Standard API, data models, etc) on which End Products can be developed.

Regional Restrictions:
Services available only in Montreal region:
- Healthcare API
- Healthcare API De-Identification
- Cloud Life sciences
- Healthcare NLP

○ Hybrid and Multi-Cloud

- Cloud Build - Service for executing builds on Google Cloud infrastructure.
- Apigee API Management - API management, development, and security platform.

Privacy Impact:
These are called out elsewhere and will be referred to in the primary references (Developer tools and API Management respectively).

Appendix B: Compliance References

Provided by Google

Customers can request for the following compliance reports from Google Cloud's Compliance Reports Manager or reach out to the Sales team.

- 2022 Google Cloud ISO 27001 Statement of Applicability (Fall)
- 2022 Google Cloud ISO 27017 Statement of Applicability (Fall)
- 2022 Google Cloud ISO 27018 Statement of Applicability (Fall)
- 2022 Google Cloud SOC 2+ CSA Start Type II Audit Report (512021-4302022)
- Google Cloud ISO 27001 Certificate March 2022
- Google Cloud ISO 27017 Certificate March 2022
- Google Cloud ISO 27018 Certificate March 2022
- Google Cloud ISO 27701 Certificate March 2022
- Google Cloud Fall 2021 Google Cloud SOC 2 Type II Report (1112021-10312022)
- Google Cloud SOC 3 Report (1112021-10312022)
- Google Cloud Onboarding_100_v1
- Healthcare_L100_Videos
- List of Google Cloud Services: https://cloud.google.com/products
- PIPEDA Questionnaire, March/April 2022
- CHI Assessment Questionnaire

Google's Public Documents

- Medical Natural Language Processing
- Healthcare Data Engine
- Google Cloud Whitepaper 2020: Ontario's Personal Health Information Protection Act