Google Cloud

Google Cloud Whitepaper
October 2023

Ontario's Personal Health Information Protection Act

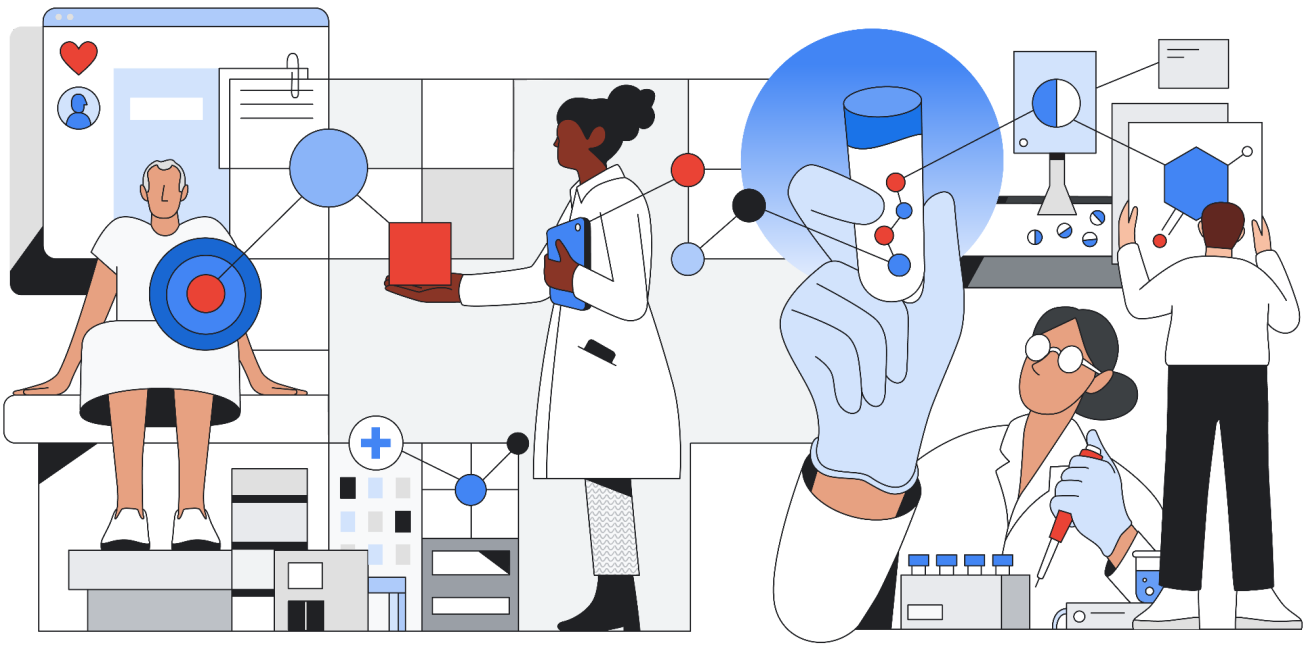


Table of Contents

Introduction **3**
Personal Health Information Protection Act (PHIPA) Overview **4**
Regulatory Environment for Ontario Healthcare Data 4
Personal Health Information 4
Health Information Custodians and Agents 4
Electronic Service Providers and Health Information Network Providers 5
PHIPA Considerations 5
Privacy Governance 5
Access and Correction Rights 6
Data Breach Management 6
How Google Cloud Helps Protect Personal Health Information **7**
Google Cloud's Approach to Privacy and Security 7
Privacy 7
Security 7
The Shared Fate Model 7
Google Cloud in the Context of PHIPA 8
Privacy Governance 9
Consent 11
Access and Correction Rights 11
Data Breach Management 12
Security Products and Services 17
Conclusion **20**
Appendix A: PHIPA Mapping **21**

Disclaimer

This whitepaper applies to Google Cloud products described at cloud.google.com. The content contained was updated as of October 2023. Google's security policies and systems may change going forward, as we continually improve protection for our customers

Introduction

The healthcare industry is benefitting immensely from the latest information technology trends. Technologies such as cloud computing, machine learning, and artificial intelligence are driving innovation in patient care delivery as more data can be collected and analyzed than ever before. Ensuring the protection of this data, especially personal health and research information, is critical and can be a major concern to those handling such data.

As a general trend, healthcare organizations continue to face cyber risks such as ransomware, phishing/spear phishing, third-party/partner breaches, data breaches, and social engineering[1]. These risks are accompanied by others such as unauthorized access, improper use, and unintentional disclosure of sensitive information by employees and third-parties. In the IAPP's 2023 Privacy Risk Study, 93% of organizations indicated privacy is a top-10 organizational risk - 36% reported it was a top-5 risk[2]. Of concern, is the emerging risk of maintaining compliance across various regulatory regimes and their evolving requirements.[3]It can be challenging to demonstrate how an organization meets the requirements outlined in Canadian regulations such as Personal Information Protection and Electronic Documents Act (PIPEDA) and provincial regulations such as Ontario's Personal Health Information Protection Act (PHIPA) .[4] Organizations are required to implement a wide range of security, compliance, and data protection practices, from robust physical security to ensuring only authorized personnel have access to personal health information. Implementing these practices in-house to safeguard personal health data can be complicated. Cloud-based solutions, such as those offered by Google Cloud, offer a scalable and economical way for organizations to implement data security and privacy controls. Google Cloud is committed to the responsibilities we share with our customers for data security and privacy and we support customers in their compliance journey with applicable laws and regulations.

In this whitepaper, we provide an introduction to Google Cloud and how it is well suited to enable organizations to address today's challenges. In addition, we provide information to help customers understand Ontario's PHIPA and how Google Cloud leverages state-of-the-art data privacy and security capabilities to store, process, maintain, and secure customer content. We are committed to showing our customers how they can deploy workloads using Google Cloud and Google Workspace for their productivity needs and benefit from the security tools and features available in Google Cloud. We explain these data protection features and how they align to many of the security and privacy practices organizations should consider when looking to comply with PHIPA.

---

[1] Health-ISAC Report Explores Current and Emerging Cyber Threats to the Healthcare Sector (April 2023) Retrieved from https://h-isac.org/health-isac-report-explores-current-and-emerging-cyber-threats-to-the-healthcare-sector/
[2] Privacy Risk Study 2023 Executive Summary (June 2023). Retrieved from https://iapp.org/resources/article/privacy-risk-study-summary/
[3] Privacy Risk Study 2023 Executive Summary (June 2023). Retrieved from https://iapp.org/resources/article/privacy-risk-study-summary/
[4]Google Cloud and Canadian Personal Information Protection and Electronic Documents Act (PIPEDA). (2018). Retrieved from https://cloud.google.com/security/compliance/pipeda_googlecloud_whitepaper

Personal Health Information Protection Act (PHIPA) Overview

Regulatory Environment for Ontario Healthcare Data

Information about an individual's health and healthcare is particularly sensitive in nature and is protected by a number of privacy regulations in Canada. In addition to the federal regulations, Canadian provinces maintain their own privacy laws. This paper focuses on Ontario's PHIPA, which came into effect on November 1, 2004.[5] The Information and Privacy Commissioner of Ontario (OIPC) is the regulator that oversees compliance for PHIPA. This section gives an overview of privacy requirements outlined in PHIPA that apply to organizations that provide healthcare services to individuals in the province of Ontario and their agents.

Personal Health Information

PHIPA establishes general principles for the collection, use, and disclosure of personal health information (PHI). It also outlines comprehensive information practices for handling PHI including security, retention, and access.[6] PHI, as defined under PHIPA includes all information relating to an individual's physical or mental health, including family medical histories, information about health services received, and other pertinent health data collected during treatment. Other information such as health identifiers, eligibility of coverage or care, and payment information could also be included as PHI under the definition outlined in PHIPA.[7]

Health Information Custodians and Agents

PHIPA requires health information custodians (HICs) and their agents to follow certain security and privacy practices in order to protect PHI and maintain the privacy of Ontario residents.[8] PHIPA's definition of health information custodians (HICs) generally includes caregivers, healthcare practitioners, and health service providers who have custody or control of PHI.[9] PHIPA requirements may also extend to individuals and organizations that receive PHI to act on behalf of a HIC as part of

[5]Frequently Asked Questions Personal Health Information Protection Act. (2015, September). Retrieved from https://www.ipc.on.ca/wp-content/uploads/2015/11/phipa-faq.pdf
[6]A Guide to the Personal Health Information Protection Act. (2004, December). Retrieved from https://www.ipc.on.ca/wp-content/uploads/Resources/hguide-e.pdf
[7]Personal Health Information Protection Act, Part 1, Section 4 - Personal health information. (2004). Retrieved from https://www.ontario.ca/laws/statute/04p03#BK5
[8]A Guide to the Personal Health Information Protection Act, pg. 4. (2004, December). Retrieved from https://www.ipc.on.ca/wp-content/uploads/Resources/hguide-e.pdf
[9]Personal Health Information Protection Act, Part 1 Section 3 - Health information custodian. (2004). Retrieved from https://www.ontario.ca/laws/statute/04p03#BK4

their role, such as a document destruction/shredding service. These individuals or organizations may be defined as an "agent" of a HIC and are also subject to certain PHIPA requirements.[10]

Electronic Service Providers and Health Information Network Providers

The OIPC has provided guidance for some types of agents, notably electronic service providers (ESPs) and health information network providers (HINPs). An ESP supplies services that enable a HIC to collect, use, modify, disclose, retain, or dispose of PHI electronically. A HINP, a type of ESP, provides electronic services to multiple HICs that communicate personal health information between them.[11]

PHIPA restricts an ESP's use and disclosure of personal health information it may have access to when providing IT services to a HIC. HINPs are subject to additional requirements under PHIPA, such as performing privacy impact assessments, reporting privacy breaches to HICs, and providing HICs with reports about the access and transfer of personal health information.[12]

PHIPA Considerations

Modern healthcare is a complex system that often involves many parties. Hospitals, outpatient centers, and pharmacies are a few types of organizations that rely on personal health information to provide quality patient care. As organizations share or control this type of data, they should ensure compliant privacy and security practices are in place to prevent incidents including unauthorized access, collection, use, disclosure, or disposal of personal health information.[13] This section provides an overview of the privacy rights and responsibilities of both organizations and individuals under PHIPA.

Privacy Governance

The OIPC recommends that organizations looking to comply with PHIPA should employ a number of measures to safeguard personal health information, including but not limited to:

- Establishing information handling practices that provide administrative, technical, and physical safeguards for the privacy of personal health information.
- Implementing privacy governance practices, such as designating a publicly reachable privacy contact and publicizing the organization's privacy policy related to the collection, use, and disclosure of personal health information.

---

[10]A Guide to the Personal Health Information Protection Act, pg. 3. (2004, December). Retrieved from https://www.ipc.on.ca/wp-content/uploads/Resources/hguide-e.pdf

[11]Frequently Asked Questions Personal Health Information Protection Act, pg. 10-11. (2015, September). Retrieved from https://www.ipc.on.ca/wp-content/uploads/2015/11/phipa-faq.pdf

[12]Frequently Asked Questions Personal Health Information Protection Act, pg. 10-11. (2015, September). Retrieved from https://www.ipc.on.ca/wp-content/uploads/2015/11/phipa-faq.pdf

[13]Personal Health Information Protection Act, Part 5.1, Section 55.3 - Requirements for electronic health record. (2004). Retrieved from https://www.ontario.ca/laws/statute/04p03#BK78

- HICs providing tailored privacy training and awareness activities to staff to ensure compliant privacy practices are used when handling personal health information.

HICs rely on patients' health information to provide high quality, personalized care, and they must protect this information to safeguard patients and maintain their trust. Under PHIPA, individuals have the right to consent to the collection, use, and disclosure of their personal health information. For further details on consent and custodians' obligations related to PHIPA, see Frequently Asked Questions Personal Health Information Protection Act.

Access and Correction Rights

PHIPA grants individuals control over their personal health information, including how they may access or amend their data. For example, an individual may submit an access request to a HIC to receive a copy of their personal health information. Individuals may also submit requests to HICs to amend their personal health information for the purposes of improving the accuracy or completeness of a record.

Data Breach Management

A privacy breach is an incident where personal health information is "stolen, lost, or accessed by unauthorized entity persons."[14] The OIPC provides regulatory guidance and enforcement against such violations. PHIPA violations[15] can carry monetary and reputational repercussions. As such, HICs must ensure they have sound administrative, technical, and physical safeguards in place to protect personal health information.

The OIPC recommends that organizations have protocols in place that address identification, containment, notification, investigation, and remediation of actual or suspected privacy breaches. Under PHIPA, HICs are responsible for notifying the individual(s) affected without undue delay; in certain circumstances, the OIPC must be notified. Agents, and HINPs may also have reporting duties in the event of a privacy breach and are typically obligated to notify the corresponding HIC(s) to the affected personal health information.[16]

At Google Cloud, we recognize that the healthcare information custodian (HIC) has the ultimate responsibility for a privacy breach incident. Nonetheless, we have built a robust program to help our customers with all data incidents regardless of the content. Please refer here for more information about our incident management process.

[14]Frequently Asked Questions, Personal Health Information Protection Act, pg. 14. (2015, September). Retrieved from https://www.ipc.on.ca/wp-content/uploads/2015/11/phipa-faq.pdf

[15]Information and Privacy Commissioner of Ontario, Potential Consequences of a Breach under PHIPA. Retrieved from https://www.ipc.on.ca/health-organizations/responding-to-a-privacy-breach/potential-consequences-of-a-breach-under-phipa/

[16]Information and Privacy Commissioner of Ontario, Reporting a Privacy Breach to the Commissioner. (2017, September). Retrieved from https://www.ipc.on.ca/wp-content/uploads/2019/09/2019-health-privacy-breach-notification-guidelines.pdf

How Google Cloud Helps Protect Personal Health Information

This section outlines the security and data protection aspects of Google Cloud's underlying infrastructure and operations. When customers build on Google Cloud, they benefit from both the security features inherent in the platform and the growing list of security features we provide to help them protect their data.

Google Cloud's Approach to Privacy and Security

Privacy

Privacy is fundamental to Google Cloud. We go to great lengths to protect the data customers store, process, and/or transit using our services. We incorporate strong privacy controls into the design and operation of Google Cloud products and services. The Google privacy team participates in every product launch, reviewing design documentation and performing code reviews to ensure that privacy is embedded in the development of each product. They help to ensure Google Cloud products and services always reflect strong privacy standards by protecting personal health information within your custody and control. We understand how important data is to your organization. We are committed to protecting your data and giving you control over how you use and share your data. For more information about our commitment to the privacy of your data, refer to the Google Cloud privacy resource center page.

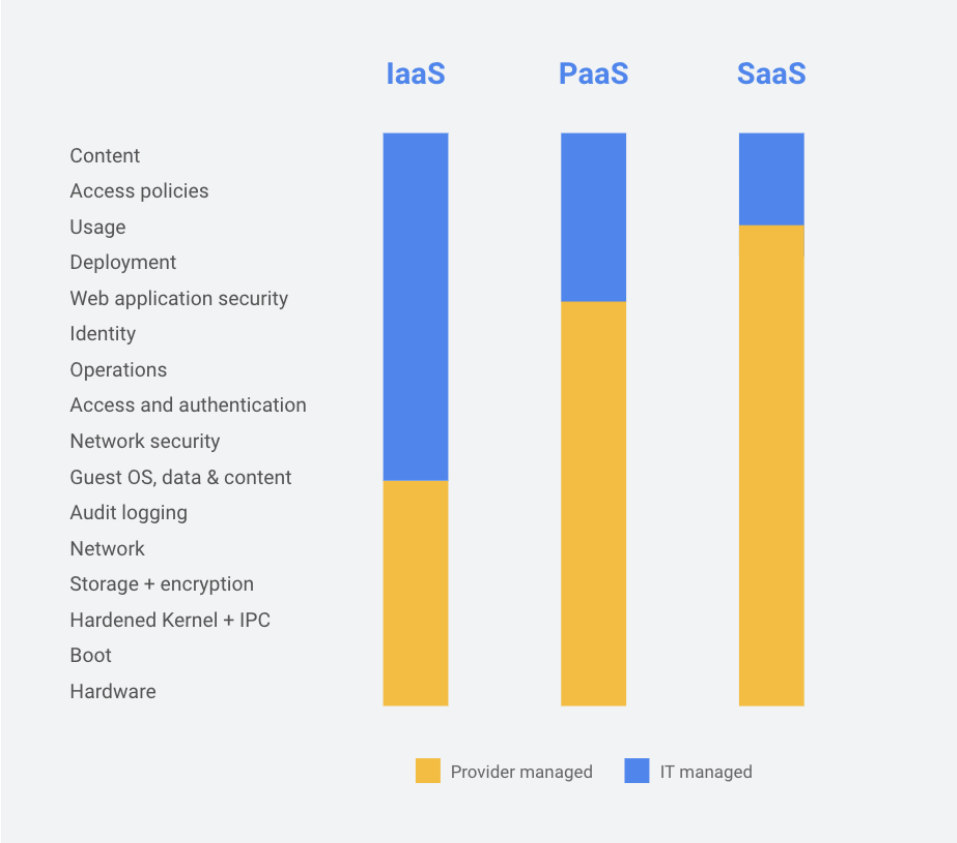
Security

Google Cloud was conceived, designed, and built to operate securely and is an innovator in hardware, software, network, and system management technologies. Security is central to Google's culture. It is reinforced in employee security training and company-wide events to raise awareness and drive innovation in security. Google continues to expand its renowned security team to explore new areas of research and innovation. As of the publishing of this whitepaper, we employ more than 850 security and privacy professionals worldwide, including some of the world's foremost experts. This team maintains our organization's defense systems, develops security review processes, designs and helps build security infrastructure, implements Google's security policies, and actively scans for security threats. Refer to the Google security whitepaper to learn more about our dedicated security and privacy teams.

The Shared Fate Model

Under a traditional Shared Responsibility Model, the cloud customer and its CSP share the responsibilities of managing the IT environment, including those related to security and compliance. Understanding shared responsibility, however, can be challenging. The model requires an in-depth

understanding of each service you utilize, the configuration options that each service provides, and what the cloud provider does to secure the service. Google believes that the shared responsibility model stops short of helping cloud customers achieve better security outcomes. Instead of shared responsibility, we believe in shared fate.



Google Cloud's role in the Shared Fate Model builds on the traditional shared responsibility. It includes us building and operating a trusted cloud platform for your workloads. We also provide best practice guidance and secured, attested infrastructure code that you can use to deploy your workloads in a secure way. We release solutions that combine various Google Cloud services to solve complex security problems and we offer innovative options to help you measure and mitigate the risks that you must accept. Shared fate involves us more closely interacting with you as you secure your resources on Google Cloud.

Google Cloud in the Context of PHIPA

As organizations that collect, use, and disclose Ontario personal health information look to adopt cloud services, they should consider a cloud service provider's experience in providing a wide range of privacy and security best practices. This whitepaper will help our customers determine how they could use Google Cloud service offerings when PHIPA or other similar applicable regulatory obligations are present. This section addresses critical areas to consider when conducting an assessment of Google Cloud products and services as it relates to PHIPA.

Our commitments to you about your data

Your data is critical to your business, and you take great care to keep it safe and under your control. We want you to feel confident that taking advantage of Google Workspace and Google Cloud services doesn't require you to compromise on security or control of your business's data.

At Google Cloud, we believe that trust is created through transparency, and we want to be transparent about our commitments and what you can expect when it comes to our shared

responsibility for protecting and managing your data in the cloud.

When you use Google Cloud, you can:

1. Know that your security comes first in everything we do.

   We promptly notify you if we detect a breach of security that compromises your data.

2. Control what happens to your data.

   We process customer data according to your instructions. You can access it or take it out at any time.

3. Know that customer data is not used for advertising.
   You own your data. Google Cloud does not process your data for advertising purposes.

4. Know where Google stores your data and rely on it being available when you need it.

   We publish the locations of our Google data centers; they are highly available, resilient, and secure.

5. Depend on Google's independently-verified security practices.

   Our adherence to recognized international security and privacy standards is certified and validated by independent auditors — wherever your data is located in Google Cloud.

6. Trust that we never give any government entity "backdoor" access to your data or to our servers storing your data.

   We reject government requests that are invalid, and we publish a transparency report for government requests.

   See the Cloud Data Processing Addendum for further details.

   To learn more, refer to the Google Cloud privacy resource center.

Privacy Governance

We are committed to protecting our customers' data and providing the administrative, technical, and physical safeguards to help address challenges around privacy governance; this commitment is demonstrated in the following ways:

- **Our commitment to protecting the privacy of our customer's data**

  Data is critical to our customers; they take great care to keep it safe while it is under their custody and control. At Google, we believe trust is created through transparency, and we want to be open about our commitments and what our customers can expect when it comes to our shared responsibility for protecting and managing the data they store, transmit, or process using our services. Our investments in security and our contractual obligations to our customers provide them with powerful, reliable, available and secure cloud services for their

own benefit. We offer our customers a detailed Cloud Data Processing Addendum that describes our commitment to protecting their data.

Customers are responsible for complying with applicable legal and regulatory requirements, including those of PHIPA. A list of products and services that can help customers meet these compliance requirements can be found below. To learn more about our commitments to safeguarding customer data, refer to the Google Cloud privacy resource center.

- **Privacy assessment support**

  Organizations should employ administrative safeguards to uphold the security of personal health information. To support your need to do privacy assessments, we maintain and provide the following documentation: ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, ISO 27701 certifications; and SOC 2 and SOC 3 reports. We engaged an independent third party to conduct a Privacy Impact Assessment (PIA) and Threat Risk Assessment (TRA) of Google Cloud to ease the process, cost and resources of conducting your due diligence. Refer to our Compliance resource center page for more information.

- **Built-in technical controls**

  PHIPA requires organizations to apply technical controls to ensure the security of personal health information in their custody or control. Google Cloud is committed to providing a secure platform for our customer's data, especially highly sensitive data such as personal health information. Our native security and data protection features recently earned us recognition as a Leader for Public Cloud Platform Native Security by Forrester.

  Google encrypts data at rest and encrypts data in transit, by default. We use several methods of encryption, both default and user configurable. The type of encryption used depends on the OSI layer, the type of service, and the physical infrastructure component. Also by default, we encrypt and authenticate all data in transit at one or more network layers when data moves outside physical boundaries not controlled by or on behalf of Google.

  Customers can benefit from the security features inherent in the platform and available to them when building on Google Cloud services and Google Workspace. While we implement numerous protections for customer data, customers bear responsibility for meeting the legal requirements that apply to them, including the manner in which they configure and use Google Cloud products to collect, use, or disclose sensitive information.

- **Our state-of-the-art data centers and physically secure infrastructure**

  Organizations are required to implement physical safeguards to protect personal health information. For example, physical access to systems that store personal health information should be restricted and only authorized personnel should be involved in the disposal of devices containing personal health information. As organizations look to provide physical safeguards for

personal health information, using Google Cloud provides the benefit of building solutions on top of a highly secure, Google-managed infrastructure.

Google's data centers feature multiple layers of physical security protections, such as biometric identification, metal detection, vehicle barriers, and custom-designed electronic access cards, 24/7/365 video surveillance, and experienced security guards. To learn more about our data center innovation, refer to our global infrastructure page.

Google Cloud runs on the same Google infrastructure that supports multiple of Google's own billion-user applications. We custom design our servers, proprietary operating system, and geographically distributed data centers. Using the principles of defense in depth, we have created an IT infrastructure that is more secure and easier to manage than most other deployment options, including traditional on-premise technologies. To learn more about our trusted infrastructure, refer to the Google Infrastructure Security Design Overview.

Depending on the Google Cloud service, we share additional responsibilities with our customers who retain responsibility for securing any on premise or third party services that they use.

Consent

Under PHIPA, HICs are responsible for requesting and obtaining consent to the collection, use, and disclosure of personal health information; Google Cloud provides functionality to help our customers request and obtain this consent as described below. For more information, please refer to the Cloud Data Processing Addendum and the Google Cloud Platform Terms of Service.

- **Developer Tools**

  Our customers can build web application(s) that acquire an end user's consent using offerings such as Google Compute Engine, Google App Engine, Google Kubernetes Engine, and Firebase.

- **Consent mechanisms**

  Customers building applications on Google Cloud can build a dialog or settings toggle to offer individuals the opt-in to a service including the data collection that comes with it.

Access and Correction Rights

Individuals have the right to access, correct, and in some circumstances, ask for the removal of or amend data held by organizations subject to PHIPA. This is a responsibility we support by providing the tools to permit our customers to readily locate, update and remove personal health information:

- **Data access and customer control**

  When customers build on Google Cloud, they do not relinquish control of who has access to their organization's data. We process our customers' data in accordance with our contractual obligations and provide customers with solutions that allow granular control and give customers the ability to audit access. Our customers can use administrative consoles such as the Cloud Console for Google Cloud and Admin Console for Google Workspace to help access,

search, correct, and remove any data they and their users host in Google Cloud. Our customers can also utilize our Access Transparency tool to audit cloud provider access(es) and thereby expand visibility and control over their content.

- **Data correction functionality**

  Our customers have full control over their data in Google Cloud and can amend it at any time. Our customers can use the Google Cloud and Google Workspace administrative consoles and services functionality to help access and rectify any data they and their users put into our systems. This functionality will help them fulfill their obligations to respond to requests from individuals to exercise their data correction rights under PHIPA. To learn more, refer to our Cloud Data Processing Addendum.

Data Breach Management

- **Customer notification**

  We have a mature process for promptly notifying affected customers in the event of a security incident, in line with Google's commitments in our Cloud Data Processing Addendum and customer agreements. Because we do not assess the contents of our customers' data, customers are responsible for the personal health information they choose to store on Google Cloud and for complying with data breach notifications under PHIPA. Customers may rely on a number of Google Cloud products and services that may help them with their notifications requirements including the Cloud Security Command Center for Google Cloud and the Alert Center for Google Workspace.

The table below shows how the controls mentioned in the Google security whitepaper map to PHIPA. See Appendix A for the text of the sections of PHIPA.

Control	*PHIPA section number*	*How Google Cloud Platform supports PHIPA Compliance*
Encryption at Rest and in Transit:	Section 12(1) - security Section 13(1) - Handling of records	Google Cloud automatically encrypts customer content at rest. Customers have options to supply their own encryption keys and to manage the keys' lifecycles. As traffic flows through Google's managed infrastructure, Google Cloud automatically employs various protections for data in transit, and also permits customers to apply additional protective layers, such as those provided by HTTPS and SSL Proxy Load Balancers.

Cloud Logging	Section 11 - Accuracy	Google Cloud automatically enables administrative and system-event logging to support the obligation to monitor for changes to personal health information, and be able to ensure accuracy. Admin Activity and System Event logs capture events that occur when changes are made to either resource configurations or metadata. Admin Activity is generated by human users, while System Event logs are generated by Google systems.
Data Loss Prevention Strategies	Section 11 - Accuracy Section 55.3 - Requirements for electronic health records	Customers that process personal health information or other sensitive data can use custom or 'shielded' virtual machine images to contain data. These images include security monitoring tools and/or have reduced attack surfaces to help protect the confidentiality and integrity of personal health information. Cloud Data Loss Prevention (DLP) aids in the detection and obfuscation of personal health information. Cloud DLP has over ninety data type detectors (e.g. date of birth, gender, person's name) that span global or regional use cases (e.g. OHIP Number). Customers can also add their own custom detectors to match data patterns unique to their business (e.g. customer identifier patterns). Developers can embed Cloud DLP into their workloads to detect the presence of sensitive data that resides inside structured or unstructured text or within images that end users upload to applications. Cloud DLP can also scan storage repositories such as Cloud Storage or BigQuery for the presence of sensitive data. Once detected, customers can leverage the included tools to transform or redact sensitive data in a variety of ways. An additional consideration for organizations that process or store personal health information or other sensitive data is to establish VPC Service Controls. VPC Service Controls offer defense-in-depth to limit data exfiltration opportunities. Network administrators can define a boundary around the VPC that specifies which hosts outside the perimeter are authorized to connect to protected resources. VPC Service Controls also dictate to which hosts outside the perimeter protected resources may connect or transfer data.

Access Transparency	Section 11(2) - Accuracy in disclosure Section 55.2 - Electronic health records	Google's Access Transparency feature provides enterprise customers with visibility into all requests made by Google employees to access their data. For example, Access Transparency logs are created when Google Cloud's Support team accesses a customer's project in order to resolve a support ticket created by the customer. Customers can view all Google employee access to their data in Access Transparency logs. Customers can integrate Cloud Monitoring with these logs to provide near-real time alerting of data access requests. Logs will contain the resources that were accessed, the methods used to access the data, the location of the Google employee making the request, and the justification for it.
Web Security Scanner	Section 55.2 - Electronic health records	Google recommends that all customers scan their web applications on a frequent basis to detect the presence of common application vulnerabilities. To assist customers with this effort, Google Cloud offers the use of its Web Security Scanner.
Organization Policies and Constraints	Section 10(1)(2) - Information practices	Organizations can utilize organization policies to enforce the following example behaviors: ● Use of corporate-approved, trusted virtual machine images, which may contain required security monitoring tools and a reduced attack surface compared to standard images available for use. ● Skip default network creation, which may introduce overly permissive network access to resources deployed within it. ● Setting data retention timeframes within Google Cloud Storage.
Secure Image and Container Development Best Practices	Section 55.3 - Requirements for electronic health records	Customers may use Compute Engine or Kubernetes Engine to deploy workloads to Google Cloud. While Google Cloud offers a variety of base images for use, customers may also choose to deploy their own secured images for either VM or container-based workloads. Customers that process personal health information or other sensitive data should consider using custom images that contain required security monitoring tools or reduced attack surfaces to help protect the confidentiality and integrity of personal health information. Administrators can enforce the use of authorized images through the use of Organization Policies.

Identity and Access Management Best Practices	Section 12(1) - Security	Google Cloud supports the use of corporate single sign-on solutions (e.g. Okta, Ping), multi-factor authentication, and the establishment of roles and user groups for access to the hierarchy and subordinate projects and resources. In addition to user accounts, administrators and developers have an option to create service accounts. Service accounts enable resources to interact with one another securely. This eliminates the need for human users to be directly involved. Like human user accounts, identity administrators can limit what resources service accounts can use and how they use them through the use of roles. To limit what activities users can perform within Google Cloud, Cloud Identity supports the use of a number of types of roles, which can be customized. Google Cloud now offers Policy Intelligence which offers customers abilities including being able to view permissions that a user has not exercised, and that could be revoked or replaced with a more suitable role, or institute limits on the levels of access that administrators can provision, thus adding a layer of governance for the organization.
Secure VPC Networking and Firewalls	Section 12(1) - Security	Google Cloud enables developers to segment similar resources into separate Virtual Private Clouds (VPC), within which they can create separate subnets for further segmentation. Creating and managing firewall rules is a vital component of an organization's security strategy, as the attack surface can be greatly reduced through the proper application of least-privilege network access.
Cloud Identity-Aware Proxy	Section 10(1)(2) - Information practices Section 12(1) - Security	Cloud Identity-Aware Proxy (IAP) represents the means by which organizations can provision application or VM-level access to users and administrators who may be on untrusted networks, thus eliminating the need to require VPN or whitelisted access arrangements. Organizations should consider this as a means to further centralize the management and deployment of access policies for applications and resources that process or handle sensitive data or that perform mission-critical functionality. IAP also provides capabilities for recording user consent to collection of private health information and conveying the use and purpose of that data by the HIC.

Incident Response and Cloud Security Command Center **Resource Inventory Management**	Section 12(1) - Security Section 10(1)(2) - Information practices	Enterprises can use Google Cloud's Security Command Center (CSCC) to centralize risk management activities and provide a common view for many security-related services. CSCC accepts feeds from a variety of security products offered by Google Cloud - including Web Security Scanner, Cloud DLP, and Google Cloud's operations suite (formerly Stackdriver) - and by third-party partners and an organization's existing security tools. CSCC uses these sources to produce daily updates for an organization's resource inventory and changes to compliance states. Security administrators can perform the following activities within Cloud Security Command Center: ● View resource inventories and identify new, modified, or deleted assets. ● Locate where sensitive data resides based on Cloud DLP scans. ● Add security marks ("labels" or "tags") to annotate findings or assets for future action or investigation. ● View vulnerability data provided by Cloud Security Scanner. ● Identify policy violations detected by Forseti Security scans. ● View additional findings detected by other Google and customer-enabled 3rd party scanners. CSCC can alert administrators of potential incidents or violations via email, SMS, or ticketing through the use of Pub/Sub and Cloud Function integration. Alternatively, security administrators can use the REST API to integrate with existing case management or SIEM platforms.
Data Location	Section 50 - Disclosure outside Ontario	PHIPA only allows HICs and their agents to disclose personal health information outside Canada if the individual patient consents or if one of several other conditions set out in section 50 of PHIPA are satisfied. As a result, unless section 50 is satisfied, personal health information cannot be transferred to agents located outside Canada, and may not be stored on servers outside Canada. Information about Google's ability to store customer data at rest in a specific region when using certain Google Cloud services can be found in the Service Specific Terms. Google also provides customers a number of network security services including encryption in transit, as well as data security features like encryption at rest and Cloud Data Loss Prevention.

Security Products and Services

Google delivers a range of product and service offerings to help customers meet compliance requirements; we list some of these in the table below.

Category	*Offering*	*Description*	*PHIPA Customer Relevance*
Governance	Asset Tracking	Accurate, real-time global location data for fleets, assets, and devices.	Google Cloud offers these services as a means for customers that store personal health information to manage and control the configuration and use of their deployed resources.
	Cloud Console	Google Cloud's integrated management console.	
	Cloud Console Mobile App	Manage Google Cloud services from your Android or iOS device.	
	Cloud Deployment Manager	Manage cloud resources with simple templates.	
	Cloud Endpoints	Develop, deploy, and manage APIs on any Google Cloud backend.	
	Cloud Healthcare API	Standards-based APIs powering actionable healthcare insights for security and compliance-focused environments.	
	Cloud Shell	Manage infrastructure and applications from the command-line in any browser.	
	Endpoint Management	Mobile device management solution.	
	Google Cloud's operations suite	Monitoring and management for services, containers, applications, and infrastructure.	
	Cloud Monitoring	Provides visibility into the performance, uptime, and overall health of applications running on Google Cloud and AWS.	
Identity & Access Management	Cloud IAM	Fine-grained identity and access management.	Google Cloud's Identity and Access & Management solutions provide customers with the ability to fully implement their PHIPA-related segregation of duties and ensure Section 12(1) compliance across their cloud environment.
	Cloud Identity	Easily manage user identities, devices, and applications from one console.	
	Cloud Identity-Aware Proxy	Use identity to guard access.	
	Resource Manager	Hierarchically manage resources on Google Cloud.	

	Firebase Authentication	Simple, free multi-platform sign-in.	
	Google Workspace Doc Controls	Set file-sharing permissions for organizations.	
	Security keys enforcement	Prevent phishing with security keys.	
Category	***Offering***	***Description***	***PHIPA Customer Relevance***
Data Security	Cloud Data Loss Prevention	Discover and redact sensitive data.	Google Cloud Data Security offerings allow customers to detect and safeguard personal health information as well as protect confidential business information relating to their customers, intellectual property, and internal processes/procedures.
	Cloud Hardware Security Module (HSM)	Protect your cryptographic keys in a fully managed cloud-hosted HSM service.	
	Cloud Key Management Service (KMS)	Manage encryption keys on Google Cloud.	
	Encryption at Rest	Encryption at rest by default.	
	Google Workspace DLP Drive	Scan and protect Drive files using data loss prevention (DLP) rules.	
	Google Workspace DLP Mail	Scan your email traffic using DLP rules.	
Network Security	Application Layer Transport Security	Mutual authentication and transport encryption system.	Google Cloud Network Security offerings ensure a robust and reliable Cloud based solution while also safeguarding patient health data in transit through TLS-level encryption.
	Cloud Load Balancing	High performance, scalable load balancing.	
	Encryption in Transit	Default TLS encryption provided to protect data in transit between customers and Google infrastructure.	
	Virtual Private Cloud (VPC)	Manage networking functionality for your Cloud Platform resources.	
	VPC Service Controls	Define secure access zones for sensitive data in Google Cloud services.	
Infrastructure Security	Binary Authorization	Deploy only trusted containers on Kubernetes Engine.	These offerings allow customers to verify the security and integrity of the underlying infrastructure that is hosting their Google Cloud-deployed applications. This helps further ensure compliance with Sections 12(1) and
	Container Security	Secure your container environment on Google Cloud.	
	Shielded VMs	Hardened virtual machines on Google	

		Cloud.	55(3).
Application Security	Apigee	Design, secure, analyze, and scale APIs anywhere.	Google Cloud application security offerings enable customers to check for common application vulnerabilities and to secure data through identity verification, data encryption, and threat analysis.
	Cloud Security Scanner	Automatically scan your App Engine apps.	
Security Monitoring & Operations	Access Transparency	Expand visibility over your cloud provider through near real-time logs.	Google Cloud Security Monitoring & Operations products help customers maintain PHIPA compliance through logging and alerting, creating an audit trail as changes or access attempts are made to objects within the Google Cloud environment.
	Cloud Security Command Center	A comprehensive security and data risk platform for Google Cloud.	
	Cloud Logging	Store, search, analyze, monitor, and alert on log data.	
	Attack Surface Management	Discover and analyze internet assets across today's dynamic, distributed and shared environments. Continually monitor discovered assets for exposures and enable intelligence and red teams to operationalize and inform risk management.	Mandiant's Attack Surface Management and Security Validation offerings allow organizations to continually monitor assets for exposures and continuously validate and measure the effectiveness of their cyber security controls across cloud and on-premise environments, enabling intelligence and red teams to move security programs from reactive to proactive.
	Security Validation	Continuously measure and validate your security effectiveness against today's adversaries	

Conclusion

Organizations that handle electronic health personal health information from Ontario can take advantage of Google Cloud products and services to help meet their security and privacy requirements. This whitepaper describes how data is stored, processed, maintained, secured, and accessed using Google Cloud products. A more in-depth understanding of how Google Cloud and Google Workspace products work can be found in the references cited throughout the whitepaper.

Appendix A: PHIPA Mapping

Control	*PHIPA section number*	*PHIPA section description*
Encryption at Rest and in Transit	Section 12(1) - security Section 13(1) - Handling of records	S 12 (1) A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal. 2004, c. 3, Sched. A, s. 12 (1). S 13(1) Handling of records 13 (1) A health information custodian shall ensure that the records of personal health information that it has in its custody or under its control are retained, transferred and disposed of in a secure manner and in accordance with the prescribed requirements, if any. 2004, c. 3, Sched. A, s. 13 (1).
Cloud Logging	Section 11 - Accuracy	Accuracy Section 11 (1) A health information custodian that uses personal health information about an individual shall take reasonable steps to ensure that the information is as accurate, complete and up-to-date as is necessary for the purposes for which it uses the information. 2004, c. 3, Sched. A, s. 11 (1).

Data Loss Prevention Strategies	Section 11 - Accuracy Section 55.3 - Requirements for electronic health record	Accuracy 11 (1) A health information custodian that uses personal health information about an individual shall take reasonable steps to ensure that the information is as accurate, complete and up-to-date as is necessary for the purposes for which it uses the information. 2004, c. 3, Sched. A, s. 11 (1). S55.3 3. It shall make available to the public and to each health information custodian that provides personal health information to it, i. a plain language description of the electronic health record, including a general description of the administrative, technical and physical safeguards in place to: A. protect against theft, loss and unauthorized collection, use or disclosure of the personal health information that is accessible by means of the electronic health record, B. protect the personal health information that is accessible by means of the electronic health record against unauthorized copying, modification or disposal, and C. protect the integrity, security and confidentiality of the personal health information that is accessible by means of the electronic health record.

Access Transparency	Section 11(2) - Accuracy in disclosure Section 55.2 - Electronic health records	11 (2) A health information custodian that discloses personal health information about an individual shall, (a) take reasonable steps to ensure that the information is as accurate, complete and up-to-date as is necessary for the purposes of the disclosure that are known to the custodian at the time of the disclosure; or (b) clearly set out for the recipient of the disclosure the limitations, if any, on the accuracy, completeness or up-to-date character of the information. 2004, c. 3, Sched. A, s. 11 (2). s55.2 Functions of prescribed organization (2) The prescribed organization shall perform the following functions: 1. Manage and integrate personal health information it receives from health information custodians. 2. Ensure the proper functioning of the electronic health record by servicing the electronic systems that support the electronic health record. 3. Ensure the accuracy and quality of the personal health information that is accessible by means of the electronic health record by conducting data quality assurance activities on the personal health information it receives from health information custodians. 4. Conduct analyses of the personal health information that is accessible by means of the electronic health record in order to provide alerts and reminders to health information custodians for their use in the provision of health care to individuals. 2016, c. 6, Sched. 1, s. 1 (12).

Cloud Security Scanner	Section 55.2 - Electronic health record	s55.2 Functions of prescribed organization (2) The prescribed organization shall perform the following functions: 2. Ensure the proper functioning of the electronic health record by servicing the electronic systems that support the electronic health record. 3. Ensure the accuracy and quality of the personal health information that is accessible by means of the electronic health record by conducting data quality assurance activities on the personal health information it receives from health information custodians.
Organization Policies and Constraints	Section 10(1)(2) - Information practices	10 (1) A health information custodian that has custody or control of personal health information shall have in place information practices that comply with the requirements of this Act and its regulations. 2004, c. 3, Sched. A, s. 10 (1). Duty to follow practices (2) A health information custodian shall comply with its information practices. 2004, c. 3, Sched. A, s. 10 (2).
Secure Image and Container Development Best Practices	Section 55.3 - Requirements for electronic health record	S55.3 3. It shall make available to the public and to each health information custodian that provides personal health information to it, i. a plain language description of the electronic health record, including a general description of the administrative, technical and physical safeguards in place to, A. protect against theft, loss and unauthorized collection, use or disclosure of the personal health information that is accessible by means of the electronic health record, B. protect the personal health information that is accessible by means of the electronic health record against unauthorized copying, modification or disposal, and C. protect the integrity, security and confidentiality of the personal health information that is accessible by means of the electronic health record, and

Identity and Access Management Best Practices	Section 12(1) - Security	12 (1) A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal. 2004, c. 3, Sched. A, s. 12 (1).
Secure VPC Networking and Firewalls	Section 12(1) - Security	12 (1) A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal. 2004, c. 3, Sched. A, s. 12 (1).
Cloud Identity-Aware Proxy	Section 10(1)(2) - Information practices Section 12(1) - Security	10 (1) A health information custodian that has custody or control of personal health information shall have in place information practices that comply with the requirements of this Act and its regulations. 2004, c. 3, Sched. A, s. 10 (1). Duty to follow practices (2) A health information custodian shall comply with its information practices. 2004, c. 3, Sched. A, s. 10 (2). 12 (1) A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal. 2004, c. 3, Sched. A, s. 12 (1).
Resource Inventory Management	Section 10(1)(2) - Information practices	10 (1) A health information custodian that has custody or control of personal health information shall have in place information practices that comply with the requirements of this Act and its regulations. 2004, c. 3, Sched. A, s. 10 (1). Duty to follow practices (2) A health information custodian shall comply with its information practices. 2004, c. 3, Sched. A, s. 10 (2).

Incident Response and Cloud Security Command Center	Section 12(1) - Security	12 (1) A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal. 2004, c. 3, Sched. A, s. 12 (1).
Data Location	Section 50 - Disclosure outside Ontario	50. (1) A health information custodian may disclose personal health information about an individual collected in Ontario to a person outside Ontario only if, (a) the individual consents to the disclosure; (b) this Act permits the disclosure; (c) the person receiving the information performs functions comparable to the functions performed by a person to whom this Act would permit the custodian to disclose the information in Ontario under subsection 40 (2) or clause 43 (1) (b), (c), (d) or (e); (d) the following conditions are met: (i) the custodian is a prescribed entity mentioned in subsection 45 (1) and is prescribed for the purpose of this clause, (ii) the disclosure is for the purpose of health planning or health administration, (iii) the information relates to health care provided in Ontario to a person who is a resident of another province or territory of Canada, and (iv) the disclosure is made to the government of that province or territory; (e) the disclosure is reasonably necessary for the provision of health care to the individual, but not if the individual has expressly instructed the custodian not to make the disclosure; or (f) the disclosure is reasonably necessary for the administration of payments in connection with the provision of health care to the individual or for contractual or legal requirements in that connection. 2004, c. 3, Sched. A, s. 50 (1).

		Notice of instruction (2) If a health information custodian discloses personal health information about an individual under clause (1) (e) and if an instruction of the individual made under that clause prevents the custodian from disclosing all the personal health information that the custodian considers reasonably necessary to disclose for the provision of health care to the individual, the custodian shall notify the person to whom it makes the disclosure of that fact. 2004, c. 3, Sched. A, s. 50 (2).