Two Guidelines from Three Ministries (2G3M)

Google Cloud

Google Cloud

Introduction

Systems that include personal identifiable medical information (Medical PII), must comply with the following two guidelines:

1. [Guideline for Safety Management of Medical Information Systems](#)[1]
2. [Safety Management Guideline for Information Systems and Service Providers Handling Medical Information](#)[2]

These are collectively referred to as the "2 Guidelines from 3 Ministries" (2G3M). Google is committed to helping our customers meet their obligations under 2G3M by offering a secure foundation on which to build systems, tools to aid in the security of those systems and education on how to utilize these tools. This paper will explain how Google meets its obligations as well as how customers may use Google services to help meet their own obligations under 2G3M. This paper is intended to be for informational purposes only. Nothing in this whitepaper is intended to provide you with or should be used as a substitute for legal advice.

Requirements

Scope

The Guideline for Safety Management of Medical Information Systems defines compliance requirements for **users** of systems that handle medical PII such as hospitals, clinics, maternity homes, pharmacies, home-visit nursing stations, care providers, and medical information networks.

In addition, with the revision of version 6.0 (May 2023), the main text has been divided into an overview section, a business management section, a planning and management section, and the compliance requirements and associated thinking required for each intended reader in each section have been more clearly stated.

The Safety Management Guideline for Information Systems and Service Providers Handling Medical Information defines compliance requirements for **providers** of systems containing

---

[1] Version 6.0, published in May 2023 by the Ministry of Health, Labour and Welfare (MHLW)
[2] Version 1.1 Published in July 2023 Jointly published by the Ministry of Economy, Trade and Industry (METI) and the Ministry of Internal Affairs and Communications (MIC)

digitized medical PII. This includes Google Cloud services where they are used to build such a system.

These guidelines include the additional need to comply with the following regulations:

- Article 20 of the Act for the Protection of Personal Information (APPI), This defines security management measures for handling PII in order to meet the Safety Management for Medical Information Systems criteria.
- The Three Principles of Electronic Records (Authenticity, Readability and Storage Property) in accordance with the e-Document Law. In order to meet criteria for Digital Records set forth in The Guideline for Safety Management of Medical Information Systems (Chapter 7, 9)
- The External Storage Notice issued by the MHLW which defines requirements for storing Medical PII externally.
- Applications, servers, storage, etc. used to provide services should be installed in locations covered by the domestic law enforcement so that the documentation can be provided to government agencies in a smooth manner.

The Safety Management Guideline for Information Systems and Service Providers Handling Medical Information additionally requires service providers to conduct both risk management and risk communication.

In terms of risk management, the guideline requires service providers to clarify the data flow, identify risks, evaluate risks, and implement reasonable risk management measures.

In terms of risk communication, providers should disclose their risk management measures to medical institutions. This includes clarification on what actions the medical institutions can take to manage risk when using their services.

Risk Management Measures

Risk management measures required to meet these requirements can be separated into the following four categories:

(1) Organizational Security

Organizational security refers to the creation, operation and documentation of an organization structure to manage security.

(2) Personnel Security

Personnel Security refers to controls that ensure staff maintain confidentiality and are trained on security measures.

(3) Physical Security

Physical Security refers to physical access controls such as barriers, locks and related measures to restrict who can access facilities.

(4) Technical Security

Technical security refers to digital access controls such as authentication, authorization, access controls as well as other security measures including logging, encryption, data leak prevention, vulnerability management and threat detection.

Shared Responsibility Model

Google Cloud is responsible for the security of the cloud infrastructure while our customers are responsible for the security of their cloud environment. Google provides a shared responsibility model as a framework for these assumptions.

Google Cloud has a relationship with its customers but not with the customer's end users. Google Cloud is not aware of the data our customers place in GCP or Google Workspace, nor do we act as handlers of that data. The only interaction Google Cloud has with any customer data in our systems is to execute the services our customers select. Customers must take appropriate measures to secure the data they place in cloud services.

Below are common measures for each risk management category. In the sections that follow we will explain how Google Cloud provides a secure foundation covering its side of the shared security model. Then we will introduce Google Cloud products and services that help customers with each security measure so that they can comply with their side of the shared responsibility model.

Organizational Security Measures

Requirement	Security Concept
Clarify roles & responsibilities of persons involved in medical PII handling.	Identity Data Governance

Have a mechanism for detection and reporting of medical PII incidents.	[Threat Detection](#)
Maintain records of medical PII handling including access & changes	[Logging](#) [Data Governance](#)
Maintain records on medical PII under management including its nature, purpose, consent and who has access.	[Data Governance](#) [Access Controls](#)
Be able to investigate a potential leak and report to relevant authorities the facts.	[Logging](#) [Threat Detection](#)
Be able to audit medical PII handling activities	[Logging](#) [Data Governance](#)
Manage the appropriate handling of medical information by outsourced businesses	[Managing Third Supplier Management](#)

Personnel Security Measures

Requirement	Security Concept
Ensure supervision of those handling medical PII	[Logging](#) [Contracts](#) [Assurance](#)
Provide training on the handling of medical PII	[Training & Consulting](#)
Ensure employees maintain confidentiality	[Training & Consulting](#)

Physical Security Measures

Requirement	Security Concept
Implement management & restrictions on medical PII handling areas	[Infrastructure](#) [Identity](#) [Data Governance](#) [Data Transformation](#)
Put in barriers on medical PII handling areas such	[Infrastructure](#)

that access or viewing by unauthorized persons is not possible.	Data Transformation
Ensure prevention of physical theft of medical PII in storage & in transit	Infrastructure Data Transformation
Implement an irreversible method of medical PII data deletion	Data Deletion

Technical Security Measures

| Requirement	Security Concept
Limit access to medical PII to only those who need access	Identity Access Controls Data Governance Data Transformation
Limit access to minimal medical PII required for each role	Access Controls
Ensure each medical PII handler can be identified and authenticated	Identity
Implement network access controls to limit potential access	Access Controls
Utilize security technologies to protect systems from unauthorized access	Endpoint CI/CD Pipeline Partners Solutions
Maintain systems at latest secure state by auto-updates	CI/CD Pipeline Managed Services
Analyze logs and detect threats in them	Threat Detection
Continuously evaluate systems for vulnerabilities	Risk Detection
Protect medical PII in storage and transport	Data Transformation
Ensure backup of medical information and systems	Backup and Resilience

Google Cloud Security

The following sections provide more details about the services, support and technical measures introduced in the previous section "Safety Management Concept".

Security in our infrastructure

Google operates global infrastructure designed to provide state-of-the-art security through the information processing lifecycle.

This infrastructure is built to provide secure deployment of services, secure storage of data with end-user privacy safeguards, secure communications between services, secure and private communication with customers over the Internet, and safe operation by administrators. Google Workspace and Google Cloud Platform run on this infrastructure.
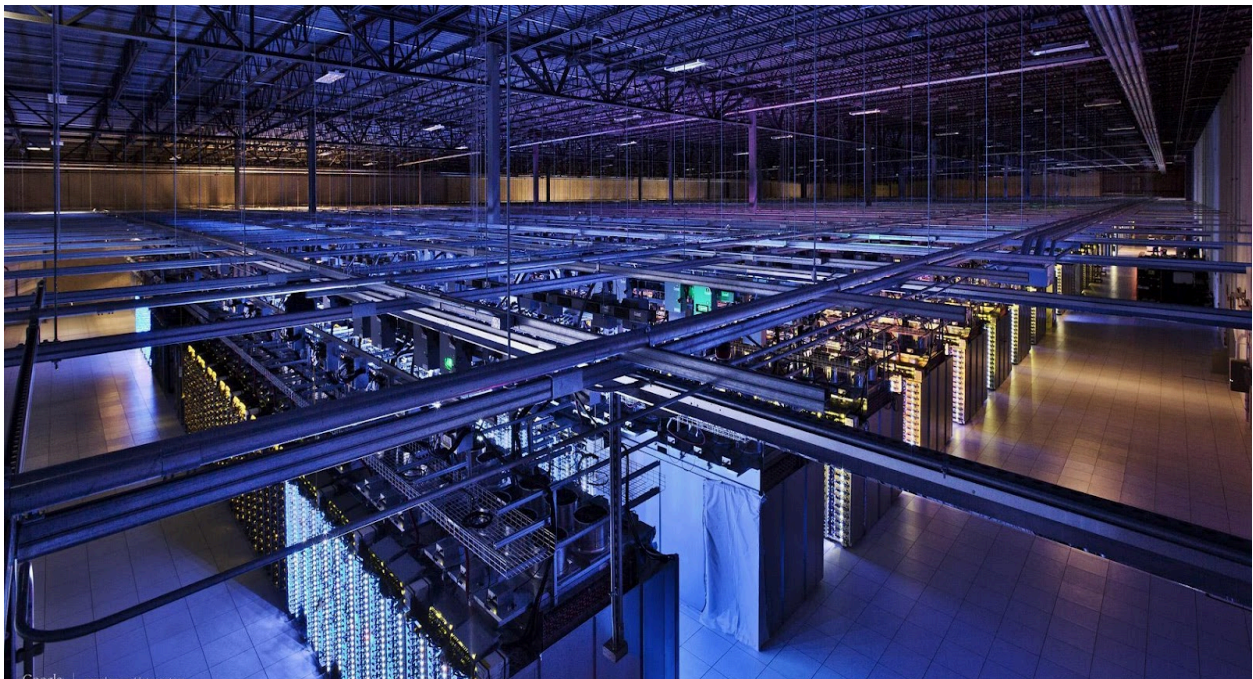
We designed the security of our infrastructure in layers that build upon one another, from the physical security of data centers, to the security protections of our hardware and software, to the processes we use to support operational security. This layered protection creates a strong

security foundation for everything we do. A detailed discussion of our Infrastructure Security can be found in our Google Infrastructure Security Design Whitepaper.

Security in our contracts

Our GCP and Google Workspace data processing terms clearly articulate our security & privacy commitments to customers. We have evolved these terms over the years based on feedback from our customers and regulators. Core to this is the understanding that any data that a customer puts into our systems will only be processed in accordance with the customer's instructions.

Google Cloud also commits to take security measures to ensure the confidentiality, integrity and availability of our systems. These are laid out in some detail in the agreement along with a further commitment that any changes we make to our security measures going forward will not degrade security. Our goal in stating this is to provide our customers continuous security improvement.

The table below shows the SLAs for some of the services in Google Cloud and Google Workspace. The SLAs for all services are published in the Google Cloud Service Level Agreement, allowing you to verify whether each Google Cloud service meets your service requirements. The table below reflects that status represents the current situation as of October 2024. Please refer to the latest information by clicking the links for each service.

Google Cloud services	Eligible Services	Monthly uptime guaranteed by SLA
Compute Engine	Instances in Multiple ZonesMulti-zone instances	99.99%
	A Single Instance of the Memory Optimized Family	99.95%
	A Single Instance of all other families	99.9%
Cloud Storage	Standard storage class in Aa multi-region or dual-region location of standard storage class in Cloud Storage	99.95%
	Standard storage in Cloud Storage regional locations, multi-region or dual-region Nearline, Coldline, and Archive storage	99.9%

	Standard storage class in a regional location of Cloud Storage; Nearline, Coldline, or Archive storage class in a multi-region or dual-region location of Cloud Storage	
	Nearline, Coldline, and Archive storage in Cloud Storage regional locations ,and highly durable, low availability storage class in any location. Nearline, Coldline, or Archive storage class in a regional location of Cloud Storage; Durable Reduced Availability storage class in any location of Cloud Storage	99.0%
Cloud SQL	Cloud SQL Enterprise Plus edition with high availability (HA)	99.99%
	Cloud SQL Enterprise edition with high availability (HA)	99.95%
Cloud Functions	-	99.95%
Google Kubernetes Engine	Zonal cluster (control plane)	99.5%
	Regional cluster (control plane)	99.95%
	Autopilot cluster (control plane)	99.95%
	Autopilot Pods in Multiple Zones	99.9%
	GKE Enterprise Autopilot Pods in Multiple Regions	99.99%

Table 2: SLA for selected Google Cloud services

Google Workspace Services	Eligible Service	Monthly uptime guaranteed by SLA
Google Workspace	AppSheet applicable services (※1)	99.99%
	Google Workspace applicable services (※2)	99.99%

Table 3: Google Workspace Service SLA

*1: AppSheet eligible services
AppSheet Enterprise Standard (purchased before June 17, 2024), AppSheet Enterprise Plus
*2: Google Workspace eligible services
Gmail, Google Calendar, Google Cloud Search, Google Docs, Google Spreadsheets, Google Slides, Google Forms, Google Drive, Google Groups for Business, Google Chat, Google Meet, Google Keep, Google Sites, Google Jamboard, Google Tasks, Google Vault, Google Voice

Security and Compliance

Google Cloud and Google Workspace undergo several independent third party audits to test for data safety, privacy, and security. Our third party audit approach is designed to be comprehensive in order to provide assurances of our level of information security with regard to confidentiality, integrity and availability. Customers may use these third party audits to assess how Google's products can meet their compliance and data-processing needs.

As a provider of cloud services to Agencies, Google complies with Information system Security Management and Assessment Program (ISMAP). Google's cloud services, including Google Cloud and Google Workspace, are registered as ISMAP certified cloud services. Please check the ISMAP Cloud Service List for details of Google services and products that are ISMAP registered.

Other major third-party certifications that Google has obtained and complies with are listed below. For more information see our Compliance Resource Center.

ISO/IEC 27001
ISO/IEC 27001 is a security standard that outlines and provides the requirements for an information security management system. The 27001 standard lays out a framework and checklist of controls that allow Google to ensure a comprehensive and continually improving model for security management. Google Cloud and Google Workspace arecertified as ISO 27001 compliant.

ISO/IEC 27018
ISO/IEC 27018 is an international standard of practice for protection of personally identifiable information (PII) in Public Cloud Services. Google Workspace and Google Cloud are certified as ISO/IEC compliant.

ISMAP
Information system Security Management and Assessment Program (ISMAP) is a government-led program to evaluate and register cloud services that meet

government security requirements. ISMAP is based on ISO27001, ISO27002, ISO270017, government uniform standards, and NIST SP 800-53. Google Workspace and Google Cloud completed the assessment for ISMAP compliance and are registered as an ISMAP compliant Cloud Service Provider. Registration details can be confirmed on the Information Technology Promotion Agency (IPA) website.

NIST SP 800-171

NIST SP 800-171 is a security standard for maintaining the confidentiality of controlled unclassified information (CUI) in non-federal information systems and organizations. The security controls in NIST SP 800-171 can be linked to NIST SP 800-53, and Google Cloud services have already undergone an independent third-party assessment to determine compliance with the NIST SP 800-53 controls that are in scope for FedRAMP, as well as all control requirements outlined in NIST SP 800-171. The services that are subject to the NIST SP 800-171 third-party assessment can be found on the Google Cloud website.

Endpoint

In order to securely handle medical PII, one must access that medical PII using a secure endpoint. At Google, we have developed browser and OS technologies as part of the Chrome product family. These products have a very small attack surface in order to prevent common threats from taking hold on an endpoint. These solutions are available to our customers as Chrome Browser, Chrome OS and ChromeBooks centrally managed by Chrome Enterprise.

Chrome Browser is a minimal browser that automatically updates itself. It uses SafeBrowsing to check URLs against a database of known bad URLs and can warn or block sites that are deemed high risk. Chrome tabs are sandboxed. Even I-frames in a tab are sandboxed. Chrome itself is isolated on the OS and has no access to other processes.

ChromeBooks run Chrome OS. Chrome OS is a read-only OS so malware has no way to infect or change the system files. ChromeBook maintains 2 copies of Chrome OS; a working copy and a standby copy. Failure to boot the working copy will pull up the standby copy. This is beneficial for upgrades which are done on the standby copy and then it becomes the working copy on reboot. So not only do you get security but you get no downtime for upgrades. ChromeBooks have a Titan-C chip that will verify the firmware, OS and browser code. Should it detect a change it will not boot that version of the OS.
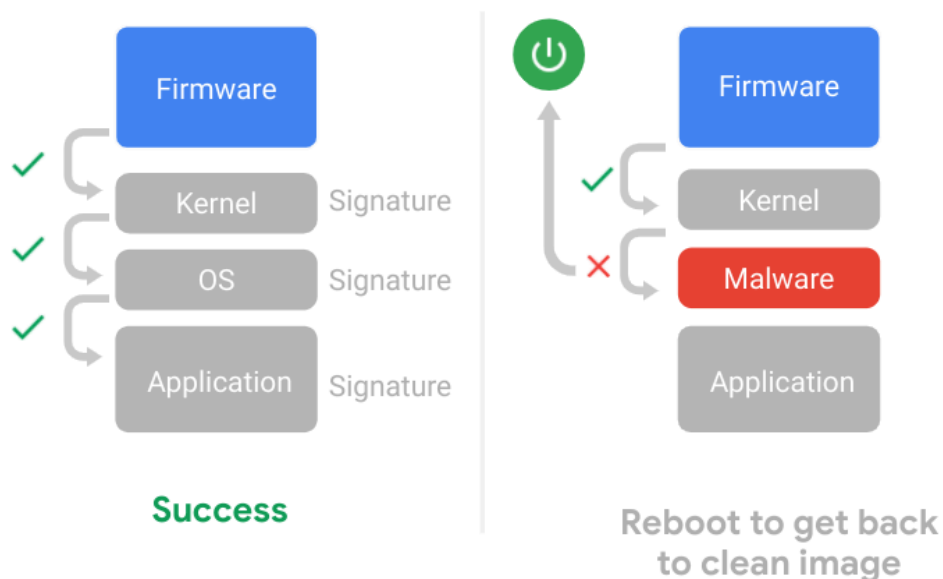
ChromeBooks encrypt data at rest but Chrome users tend not to have much data on their ChromeBooks since most of their data is in Google Cloud Services such as Google Workspace. Thus there is nothing to steal and even if ransomware could take hold, it would have nothing to ransom.

Chrome Enterprise Upgrade is a cloud based management system for having consistent administration over the Chrome OS environment. Software deployment, upgrades and Chrome settings can be configured for your entire fleet from one single console. Using Chrome Enterprise and ChromeBooks customers can easily meet and greatly exceed the PPC's expectations for security controls on the endpoint.

Identity

Identity is the backbone of access control. Google Cloud supports multiple identity providers as well as our own Cloud Identity.

Cloud Identity uses machine learning to detect unauthorized access and can even detect and block unauthorized intruders using the correct password.

Cloud Identity also supports the strongest forms of account protection including multiple 2FA options such as FIDO compliant security keys. Googlers use security keys on our own accounts to provide stronger identity protection and to prevent phishing attacks. We recommend our customers do the same.


Access Controls

In Google Cloud all services require authorization to use. Authorization is managed primarily in IAM. IAM allows you to grant roles to members such as users and groups. These roles are

made up of fine grained permissions. Curated roles are provided and customers can create custom roles as needed.

Conditions can also be applied to roles. So for example a contractor that is only supposed to work 9 to 5 can have a condition added to the roles attached to them that limits their access to just 9 to 5.

GCP has a resource manager where you can set up a folder tree to organize your projects. Access controls can be managed at any layer of the hierarchy and inherited down which is beneficial for good governance. Medical PII specific folder(s) could be established and access controls applied there so as to have them consistent across all projects in that folder.
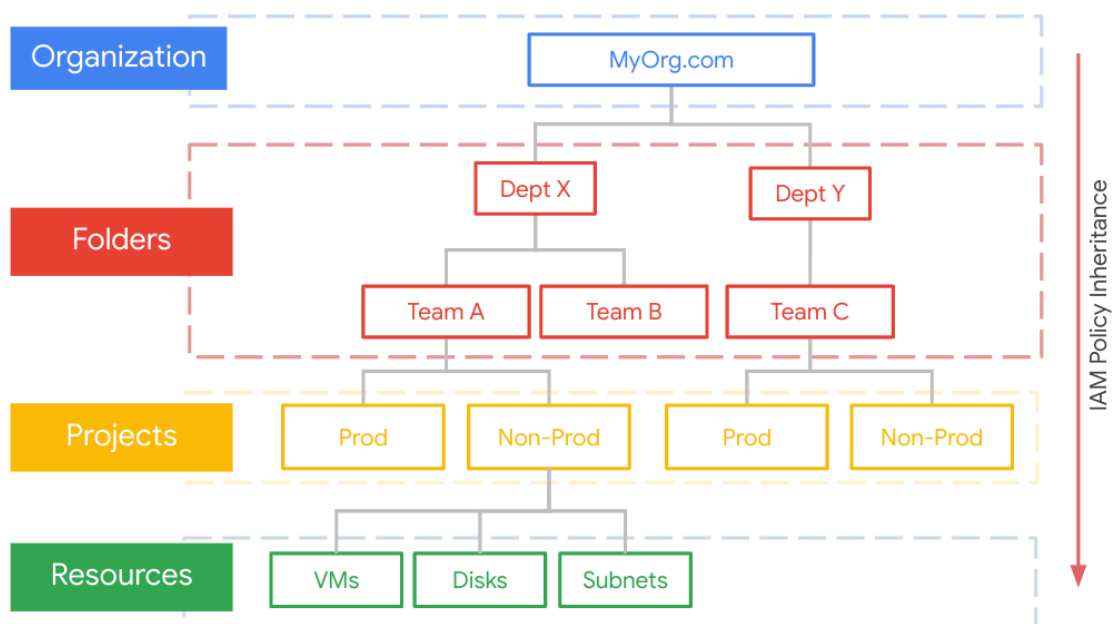
One of the biggest challenges for enterprise customers is not granting access but rather taking it away when it is not needed or excessive. IAM Recommender uses machine learning to see what permissions are being used and which are not and then makes recommendations to remove excess access. Policy analyzer can help you figure out who has access to what, which is helpful in an audit situation.

Some Google Cloud services include service specific access controls that exceed what IAM can offer. For example in BigQuery you can set up limited views of data tables and you can filter rows and columns meeting certain criteria. This can be very useful for minimizing the medical PII data analysts can see or filtering it out entirely.

In Google Workspace you can apply access controls on services based on the context of the user's identity and device. You can define at the file level who can read, comment or edit each individual file or folder.

Network Access Controls

In a traditional network, including most cloud providers, firewall rules for network access control can only be applied at choke points. In Google Cloud firewall rules are much more flexible. They can be applied to a single VM, tagged assets, assets that share the same service account or a combination of factors.

Instead of applying the same rules to every project, common rules can be applied across projects at folder or organization level using hierarchical firewall policies.

The rules affecting an asset can be analyzed both from the command line as well as in the Network Intelligence Center.

It is also important to control access to service APIs. In Google Cloud you determine what APIs you want to turn on or off. Furthermore you can place a perimeter around the APIs of your project using VPC Service Controls. VPC-SC can block data egress and place conditions on ingress.

Proper management of DNS is also important to protect your domains against spoofing and cache poisoning attacks. DNSSEC is a feature of the Domain Name System (DNS) that authenticates responses to domain name lookups. Cloud DNS supports DNSSEC, and while it doesn't not provide privacy protection for these lookups, it does prevent responses to DNS requests from being tampered with or poisoned.

Application Access Controls

Google Cloud provides the infrastructure for our customers to build their applications. The access controls inside those applications are part of the application logic the customer provides. However the access to those applications can leverage our context aware access system called Chrome Enterprise Premium.

Chrome Enterprise Premium is a zero-trust solution provided through Google's global network, enabling secure access to applications and cloud resources by protecting data from centralized threats. Zero trust is a security model used to protect organizations based on the concept that people and devices are not trusted by default, even if they are within the organization's network.

The zero-trust approach aims to eliminate implicit trust by enforcing strict identity authentication and authorization not just at the trusted perimeter, but throughout the entire network.

Chrome Enterprise Premium allows you to define which users can access which applications under which conditions. Those conditions can be related to the situation (e.g. time), the device (e.g. corporate managed) and the user's identity and authentication (e.g. MFA). This adds stronger controls that simple identity to systems with important information.

Chrome Enterprise Premium also has the ability to examine data uploads/downloads in Chrome and determine if certain data is included. It can then take a predefined action such as to block that data movement.

Logging

Google Cloud offers extensive audit logging for services. Network logs provide both network and security operations with in-depth network service telemetry. VPC Flow Logs can be used for network monitoring, forensics and real-time security analysis. Packet level capture can be done with Packet Mirroring for content analysis or to feed into a Network Intrusion Detection System. Firewall Rules Logging allows you to audit, verify, and analyze the effects of your firewall rules. NAT and DNS logs are also available for threat analysis.

Google Cloud Platform has Cloud Audit logging to log API activities including who did what, where and when. Data access logs can provide additional details at the data level and are especially useful for data management services. Google cloud does not handle customer data but if a customer specifically instructs us to access their data as part of support troubleshooting then that access is also logged and those logs can be made visible to customers via Access Transparency.

Cloud Operations provides a centralized tool for logging that can take in logs from a multitude of sources including custom logs sent from OS level agents, Fluentd, REST APIs, client libraries or 3rd party applications. Logs can be investigated and analyzed in real time with Logs Viewer., orIn addition, you can visualize and alert on your logs with logs-based metrics and Cloud Monitoring.

GCP provides a variety of log storage and retention options to meet both security & compliance requirements. System logs and data access logs are retained for 30 days by default or optionally up to 10 years. Admin logs are retained for 400 days in locked storage. Log data is immutable, encrypted at rest and monitored via Access Transparency.

Google Workspace includes extensive logging capabilities for everything from administration to users to services to devices. These logs can be fed to Cloud Operations in GCP for consolidated analysis.

Threat Detection

Security Command Center (SCC) in Google Cloud provides wing to wing risk management for Google Cloud customers. One component of SCC is threat detection. SCC will compare logs to known indicators of compromise as well as suspicious behaviors and surface alerts. Those alerts can be acted on automatically by triggering cloud functions. So for example, a VM detected to be compromised could be imaged and isolated on the network all automatically.
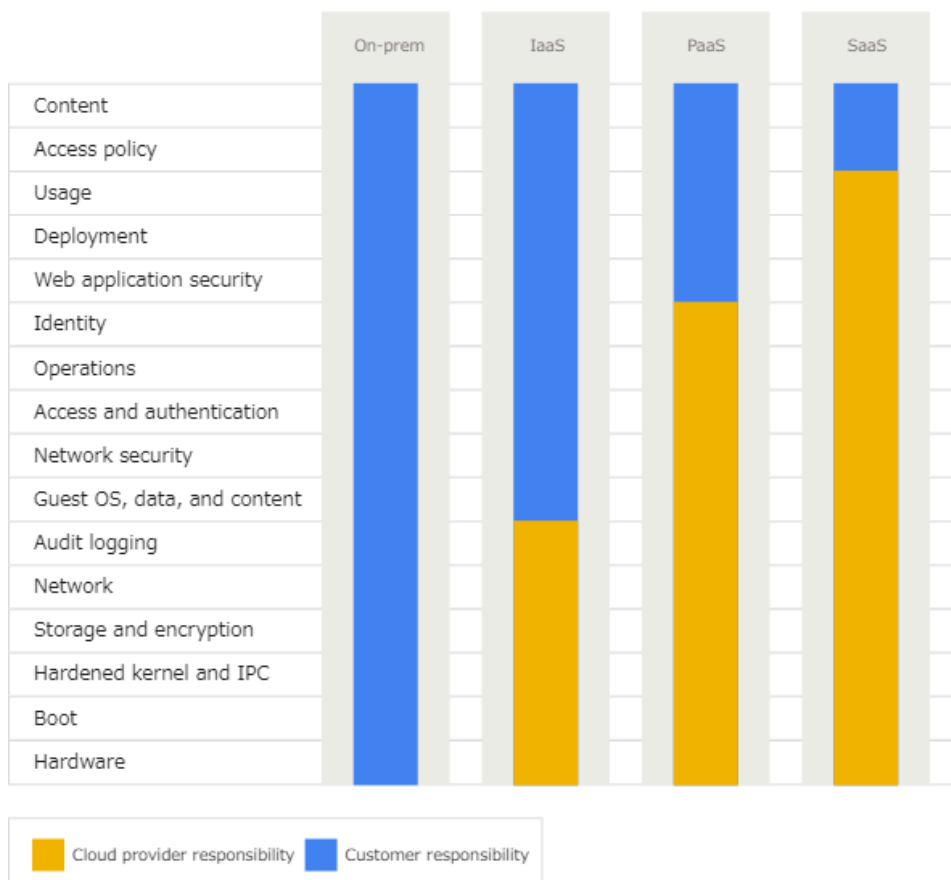
Logs can also be exported from Google Cloud to Google Security Operations SIEM or 3rd party SIEMs like Splunk for further threat analysis or correlation with non-cloud logs to see the bigger enterprise threat picture. Google Security Operations SIEM continuously compares all your logs to a huge database of indicators of compromise (IOC) and surfaces any matches. Google Security Operations SIEM can search petabytes of logs in a single second.

Google Security Operations SOAR is a platform designed to help organizations detect, investigate, and respond to security threats in real time. Google Security Operations SOAR leverages Google's machine learning capabilities to automate and streamline security workflows, allowing security analysts to investigate incidents, create workflows, and automate response actions without requiring advanced coding knowledge.

Managed Services

Maintaining systems is complicated, costly and distracting for most customers. We recommend using managed services which we maintain for you. As you can see by the diagram below the

more managed a service is the more you can focus on your data and leave the responsibility for the underlying infrastructure to Google. (Shared Responsibility Model)

	On-prem	IaaS	PaaS	SaaS
Content				
Access policy				
Usage				
Deployment				
Web application security				
Identity				
Operations				
Access and authentication				
Network security				
Guest OS, data, and content				
Audit logging				
Network				
Storage and encryption				
Hardened kernel and IPC				
Boot				
Hardware				

Cloud provider responsibility   Customer responsibility

Even in cases where compute services are required, we recommend taking advantage of the most managed form. For example a simple function can be run in cloud functions without any need for further management. Containers can be managed in GKE with node auto-upgrades which decreases the maintenance burden.

The team that manages the security of GKE is the same team that designed and wrote large parts of K8s identity, authorization and security policy code. The same team that led or contributed to the investigation, triage, patching, and notification of every serious K8s vulnerability since day 0.

Secure CI/CD Pipeline

One way a threat actor might abuse medical PII is to alter the code that is loaded into an application handling medical PII. This is why having security as part of your continuous integration and delivery pipeline (CI/CD) is so important. We recommend having a healthy code review process in place and have provided a guide to the public where we share our own practices and thoughts on this subject.

Google Cloud provides COS (Container Optimized OS) for nodes. Container-Optimized OS's small OS footprint minimizes security exposure while still containing essential built-in security features like a minimal read-only root file system, file system integrity check, locked-down firewall, and audit logging. Automatic updates patch security vulnerabilities for you and in a timely manner, further reducing your risk of compromise.

Shielded GKE Nodes is built on hardware with a Titan chip that sets off a provenance validation sequence from the host bootloader right up to the guest COS kernel in order to ensure end to end supply chain security.
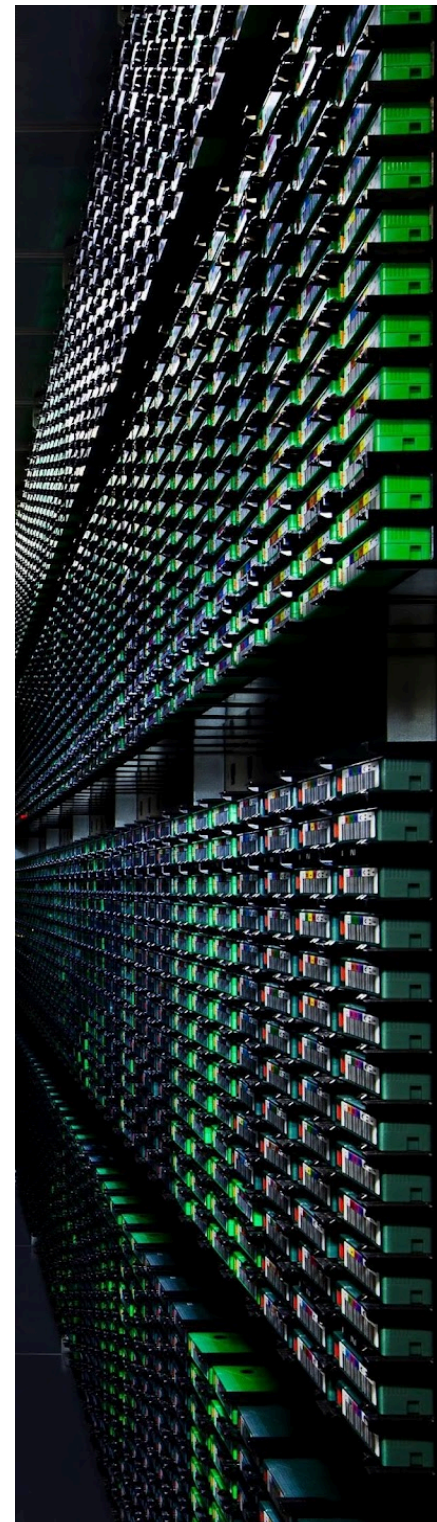
Ensuring vulnerable containers are detected and addressed is key.
Google Cloud can scan your containers added to [Artifact Registry](#)
and report any defects.

Container policies can be set using Anthos Container [Policy Controller](#). This is great for governance and can be used to ensure that a project team doesn't deploy containers with rights exceeded that allowed by company policy.

Using [Binary Authorization](#) it is possible to define signatures for passing various steps of the CI/CD pipeline and these signatures can be checked as a condition of deployment. This not only ensures all steps were passed but also keeps unauthorized code from being deployed to production.

Google Cloud infrastructure can also be managed and deployed as code. Google Cloud has published reference architectures and guides to help customers get started with these techniques. The [Google Cloud Data Protection Tool-kit Guide](#) is specifically aimed at Healthcare and Life Sciences workloads. The toolkit combines best practices and security configurations for deploying Google Cloud resources to store and process sensitive data.

Risk Detection

Application code can also be checked while running by [Web Security canner](#) which looks for common misconfigurations and vulnerabilities targeted by [OWASP](#). Our premium offering even scans GCP looking for web applications and can surface shadow applications that may have been built without authorization.

[Security Command Center](#) checks your entire Google Cloud organization for misconfigurations and vulnerabilities and then maps those against a list of your cloud assets. In fact SCC will map risks and threats not only to assets but also to different compliance frameworks such as ISO 27001, PCI DSS and the CIS best practices for Google Cloud. This allows you to meet your obligations to prevent and detect incidents affecting information you place in Google Cloud. Additionally, [Google Cloud Security Best Practices Center](#) provides best practices for achieving security and compliance goals when deploying workloads on Google Cloud, allowing customers to implement measures to prevent configuration errors

In Google Workspace you can get insights into security events and metrics that demonstrate your security effectiveness in a single, comprehensive dashboard called [Security Center](#). From there you can Identify, triage, and take action on security and privacy issues such as deleting malicious emails across your organization and examining file sharing to spot and stop potential data exfiltration.

Data Governance

Keeping track of medical PII can be a challenge for organizations as different systems and functions in the company make different copies. Data Governance is key and Google Cloud can help with this. By data governance we mean:

1. Discover medical PII
2. Label medical PII
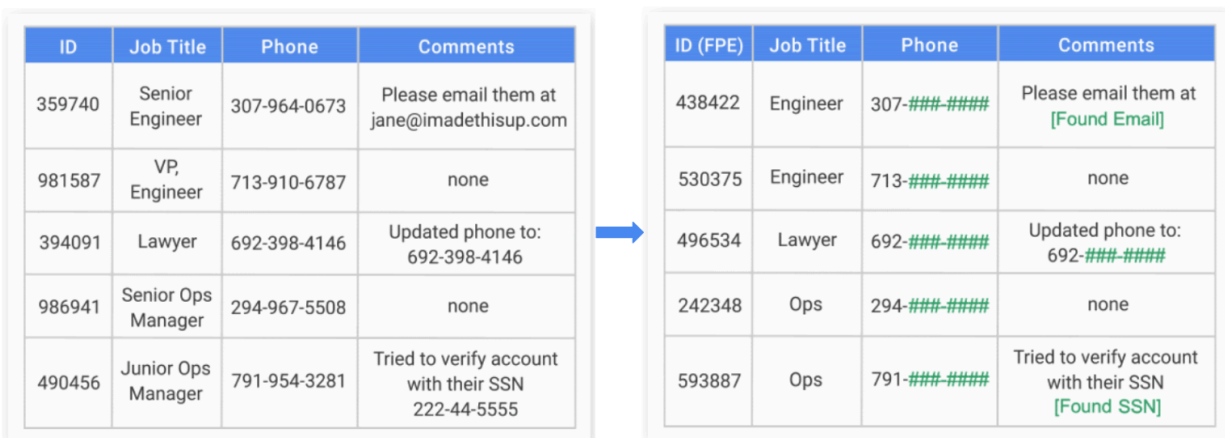3. Apply rules to medical PII

Data Catalog can use DLP API to find and apply metadata labels to your medical PII regardless of its location. Those labels can be used to apply rules so as to screen in/out certain data in processing jobs or data analytics systems.

Customers can select the region to run their workloads including two regions under Japanese jurisdiction.

Google Workspace also has DLP capabilities which administrators can configure to detect medical PII in files and take actions such as alerts or set restrictions on them such as to restrict outside sharing.

Data Transformation

Medical PII can be hidden or removed at different handling points using transformation techniques. DLP API can remove medical PII by masking or redacting the medical PII.

There may be times when you both need to use medical PII but also need to hide the medical PII. There are two ways to do that. In the case of using it as a field in a data table you can use DLP API to replace the medical PII with unique tokens (tokenization). If you only need to hide the data in storage or transit but would like to unhide it later then encryption makes more sense.

Google Cloud offers many encryption options. Cloud Key Management Service (Cloud KMS) can have cryptographic operations as a managed service that you access via an API. Additionally, You can manage customer-managed encryption keys (CMEK) with Cloud KMS,allowing you to own and control the keys used to protect your data stored on Google Cloud.

Under Cloud HSM you can use the same KMS front end knowing the backend is a FIPS-2 Level 3 certified HSM. Depending on your security requirements, you can also use your own encryption keys. In fact, you can even use the Cloud KMS front end with an External Key Manager if you wish to separate duties.

Data Deletion

Customer data in Google Cloud belongs to the customer and the customer can select to delete it at any time. Doing so makes the data immediately unavailable and kicks off wipe out procedures that extend to the various service components involved. These wipe out procedures can take up to 180 days. These procedures once complete provide for irreversible destruction of the data. Details are in the following whitepapers for GCP & Google Workspace.

Backup and Resilience

It is necessary to establish operational continuity plans for information systems and perform backups in order to continue the business operations of the organization in the event of an emergency. By using backup and disaster recovery solutions on Google Cloud, you can prepare for various threats or failures that lead to data loss.

Google Cloud products and services offer a broad range of data protection features such as Backup for GKE, Persistent Disk snapshots, Cloud SQL backups, Filestore backups, and geo-redundant Cloud Storage. You can also create and deploy Google Cloud resources across multiple regions and zones to build resilient and highly available systems.

Backup and DR Service protects a broad spectrum of workloads and manages them from a central dashboard. It also serves critical use cases such as recovery from data corruption, data loss, ransomware recovery, or database cloning for test/dev.

We design the components of our platform to be highly redundant to prevent data loss on the infrastructure managed by Google as a cloud service provider. Our data centers are geographically distributed to minimize the effects of regional disruptions on global products, such as when natural disasters or local outages occur. If hardware, software, or a network fails, platform services and control planes are automatically and swiftly shifted from one facility to another so that platform services can continue without interruption.

Our systems are designed to minimize downtime or maintenance windows for when we need to service or upgrade our platform. For more information about how Google Cloud builds resilience and availability into its core infrastructure and services, from the initial design through to ongoing operations, see Google Cloud infrastructure reliability guide.

In addition, Google Cloud Service Health Dashboard (CSH) displays status information for products included in Google Cloud. The status includes informational messages about interruptions, outages, and temporary issues. This allows customers to understand ongoing incidents, identify the causes of system failures built on Google Cloud, and organize the estimated time for recovery.

Managing Third Party Suppliers

In cases where a cloud service provider subcontracts its services, medical institutions should be careful to ensure that the service provider appropriately manages third-party suppliers.

For most data-processing activities, we provide our services in our own infrastructure. However, we may engage some third-party suppliers to provide services related to Google Cloud, including customer support and technical support.

Before outsourcing a supplier, we assess their security and privacy practices. This assessment checks whether the supplier provides a level of security and privacy that is appropriate for their access to data and for the scope of the services that they are engaged to provide. After we have assessed the risks that are presented by the third-party supplier, the supplier is required to enter into appropriate security, confidentiality, and privacy contract terms.

For more information, see the Supplier Code of Conduct.

For more information, see our Supplier Code of Conduct.Training & Consultation

Google Cloud has a wide range of training and consultation support for our customers such as:

- Pre-sales staff to walk you thru our services and help choose the right ones

- Training and education staff to train your team

- Cloud on Air and Youtube Videos

- Online training partners so you can train on your own schedule

- Certification program to level set required skills

- Online documentation in multiple languages

- Google Cloud Skills Boost to practice using our services

- Post-sales consulting services

- System integrator partnerships to build and manage solutions at scale

- A lively online community of blogs, knowledges, videos and chat rooms to share ideas and derive inspiration

Partner Solutions

Google Cloud has partnered with a wide variety of security solutions companies to make their solutions available to our customers either via the Google Cloud Marketplace or other partnership agreements. In addition we provide basic compute services that can support most security solutions regardless of whether they are a Google Cloud partner or not.

Our sales team is happy to hear your security requirements and provide consultation on which partner solutions best match your use cases.