Google Cloud Whitepaper
January 2023

Using Google Cloud in GxP Systems

Google Cloud

Table of Contents

Disclaimer

This whitepaper applies to Google Cloud products described at cloud.google.com. The content contained herein is correct as of January 2023 and represents the status quo as of the time it was written. Google's security policies and systems may change going forward, as we continually improve protection for our customers.

1.0 Introduction

Cloud computing, because of its strategic and operational advantages, is being adopted with increasing regularity by the life sciences industry. Cloud computing enables regulated organizations to use global platform solutions for data management and analysis, and presents an opportunity to more efficiently meet regulatory obligations. At Google, we understand the needs, constraints, and considerations that our life sciences customers experience with respect to migrating their workloads to the cloud. In this paper, we will describe how Google Cloud supports customers interested in utilizing the cloud to build a GxP-aligned IT environment. This includes our approach to managing quality, security and compliance for Google Cloud, and Google's organizational and technical controls to protect customer data.

What is Google Cloud?

Google Cloud is a suite of cloud services broadly categorized in infrastructure, platform, and software solutions. Alongside those services, Google Cloud offers a range of tools from smart analytics to artificial intelligence capabilities. At its core, Google Cloud consists of a set of physical assets, such as computers and hard disk drives, and virtual resources, such as virtual machines (VMs), that are contained in Google's data centers around the globe. Each data center location is in a region. Regions are available in Asia, Australia, Europe, North America, and South America. Each region is a collection of *zones*, which are isolated from each other within the region. This distribution of resources provides several benefits, including redundancy in case of failure and reduced latency by locating resources closer to clients.

In cloud computing, what you might be used to thinking of as software and hardware products, become services. These services provide access to the underlying resources. The list of available Google Cloud services is long, and it keeps growing. When you develop your website or application on Google Cloud, you can mix and match these services into combinations that provide the infrastructure or solution you need, and then add your code to enable the scenarios you want to build.

What is GxP?

In the life sciences industry, GxP is an abbreviation referencing the various "good practice" regulations and guidelines that apply to medical products. The "x" variable in GxP covers a wide range of processes utilized in the development, manufacturing, and distribution of regulated products. Particular GxP criteria can be found in government agency regulations and guidance (e.g., Federal Food, Drug, and Cosmetic Act) as well as industry best-practice frameworks. Though GxP may cover any number of specified topics, for regulatory oversight purposes, agencies have almost uniformly adopted requirements related to product manufacturing processes, documentation procedures, staff qualifications and training, and distribution/storage. For life science organizations doing business in the U.S., GxP requirements can

generally be found in the Code of Federal Regulations ("CFR").[1] These requirements include, but are not limited to:

- Good Manufacturing Practice (GMP): 21 CFR Parts 210 and 211, applicable to drug products
- Quality System Regulation (QSR): 21 CFR Part 820, applicable to medical devices
- Good Laboratory Practice (GLP): 21 CFR Part 58, applicable to nonclinical laboratory studies
- Good Clinical Practice (GCP): Includes multiple regulations and guidance applicable to scientific studies[2]
- Good Distribution Practice (GDP): Encompasses various provisions and guidelines addressed in 21 CFR Parts 211 and 820, including those related to handling, storage, and installation

GxPs were developed to ensure that medical products such as drugs, devices, and biologics are safe, meet their intended use, and adhere to quality procedures throughout the manufacturing and distribution process. This whitepaper focuses on the GxP-related topics most relevant to life science organizations, and in particular on how Google Cloud can be utilized by organizations as an element of their GxP compliance systems.

How might customers leverage cloud services in GxP Systems?

Our life sciences customers, many of whom are subject to GxP requirements, utilize Google Cloud in ways that not only help to achieve compliance, but also result in differentiated capabilities, technological advancements, and organizational efficiencies. A few representative examples include:

- **A contract research organization (CRO) uses a cloud-based project management platform hosted on Google Cloud to share trial-related information with sponsors.**

  Since this type of customer is managing a clinical trial, they are subject to good clinical practices and certain requirements aimed at protecting patients.[3] The size of clinical trials can vary greatly, with some trials only requiring the use of a few regional sites, while others may necessitate data from thousands of patients across dozens of sites globally. With Google Cloud services, users can build any number of customized applications and solutions to fit their needs. For example, by using an online workflow to onboard and track patients, a CRO could potentially eliminate the need to maintain and audit paper records physically located at each site. Google Cloud services may also help to improve compliance with clinical trial procedures by providing real-time feedback to the CRO about how sites are complying with applicable protocols. Additionally, maintaining trial data information on the cloud allows for access to the data anywhere and at any time by the appropriate teams, with greater control over user access requirements than traditional paper files.

---

[1] While the scope of this paper does not include an exhaustive international search for all applicable GxPs, it is generally true that regulatory agencies globally require medical products to be developed and manufactured in accordance with good practices. Such practices can be found directly in government regulations, guidance documents, and issued international standards.

[2] See Food and Drug Administration, *Regulations: Good Clinical Practice and Clinical Trials*, https://www.fda.gov/science-research/clinical-trials-and-human-subject-protection/regulations-good-clinical-practice-and-clinical-trials.

[3] Id.

- **A life sciences manufacturer uses a cloud-hosted interactive voice response platform to manage customer copay card requests.**

  Depending on how the platform is collecting information, the process may be subject to good pharmacovigilance, or safety reporting practices (GPvP). If the system is hosted in the cloud, the customer will have to consider how the infrastructure was qualified or determined to meet requirements. The organization may also be subject to controls that ensure that the GxP records, in this case call notes, are protected appropriately. FDA's electronic record requirements at 21 CFR Part 11 provide that any changes to data stored in electronic systems are recorded and attributable to an appropriate individual. In this paper, we outline how Google Cloud can help customers meet these requirements.

How does Google Cloud help customers comply with GxP requirements?

As an industry-leading cloud service provider, Google Cloud helps life science organizations comply with the FDA's electronic records requirements under 21 CFR Part 11 and its global equivalents.[4] Google Cloud's administrative, physical, and technical controls help our life science customers meet their quality and security objectives. In addition to the underlying infrastructure and operations managed by Google, Google Cloud products also provide capabilities which make it easier for our customers to meet applicable GxP requirements by managing their GxP recordkeeping obligations in the cloud. Google is committed to protecting its customer information and undergoes routine audits by independent third parties to verify compliance with numerous globally recognized security and data privacy standards. In fact, Forrester Research recognized Google Cloud as a Leader for Public Cloud Native Security for our security capabilities and features and as a Leader for Data Security Portfolio for our security product offerings.

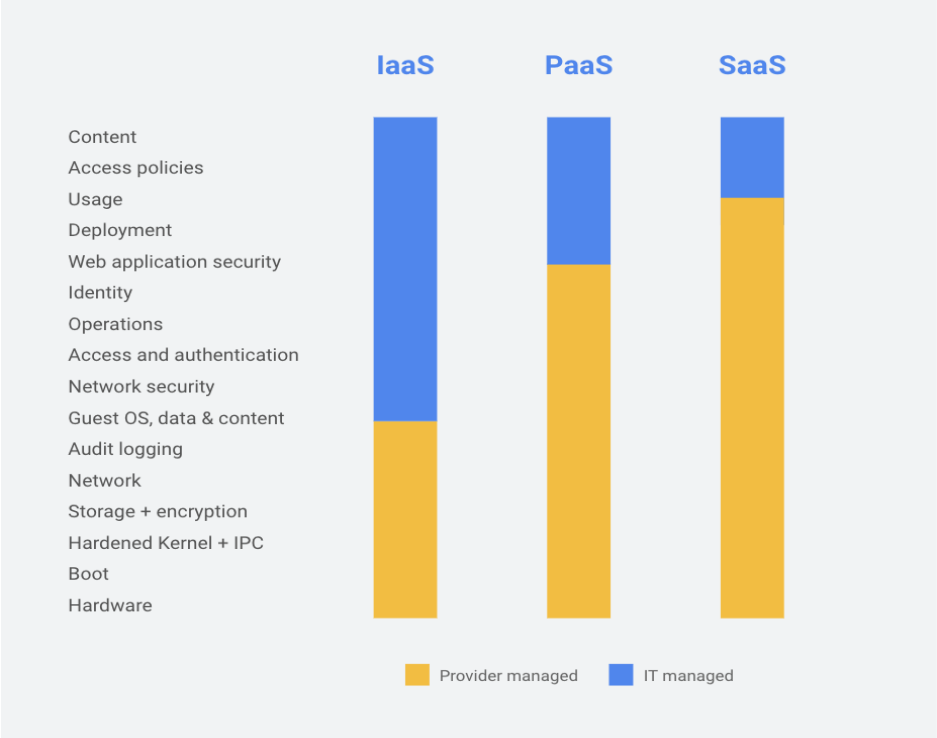
In this paper we will describe the different measures that Google Cloud takes to help customers align with GxP requirements, and also explain how life science organizations can use Google Cloud offerings in a manner that complies with the various quality and security requirements applicable to regulated industry. While references to — and details of — regulatory standards and guidance are provided as a framework for discussion, they do not constitute legal advice for pharmaceutical organizations nor for any other entities.

Shared Responsibility Model

While the responsibility for GxP compliance ultimately lies with our life science customers, our shared responsibility model helps customers allocate resources more effectively by reducing the amount of effort needed to develop and maintain an IT environment. The model helps to alleviate some of the administrative and technical burdens faced by our customers, as our tools assist with the efficient

[4] See Food and Drug Administration, (2019, May 7) *Part 11, Electronic Records; Electronic Signatures - Scope and Application*, Retrieved from https://www.fda.gov/regulatory-information/search-fda-guidance-documents/part-11-electronic-records-electronic-signatures-scope-and-application

management and control of system components that organizations subject to GxP requirements often rely upon. It also shifts a portion of the cost of security to Google Cloud, and may lower the cost of GxP compliance. As this illustrative, but not definitive, graphic shows, Google is generally responsible for securing our infrastructure and customers are responsible for securing their data. The specific responsibilities vary according to whether a customer is taking advantage of IaaS-like services on Google Cloud such as Compute Engine, PaaS-like services such as App Engine, or SaaS-like services such as G Suite. We help customers with their portion of responsibility by providing best practices, templates, products, and solutions.



2.0 Using Google Cloud in GxP Systems

As a cloud pioneer, Google fully understands the security implications of the cloud model. Our cloud services are designed to deliver better security than many traditional on-premises solutions. We make security a priority to protect our own operations, but because Google runs on the same infrastructure that we make available to our customers, your organization can directly benefit from these protections. That's why we focus on security, and protection of data is among our primary design criteria. Security drives our organizational structure, training priorities and hiring processes. It shapes our data centers and the technology they house. It's central to our everyday operations and disaster planning, including how we address threats. It's prioritized in the way we handle customer data. And it's the cornerstone of our account controls, our compliance audits and the certifications we offer our customers.

This section provides an overview of how Google Cloud's tools and approach to security and quality management can help support GxP systems of pharmaceutical and other life science organizations. In addition, we briefly summarize some elements of our suite of cloud products and capabilities that may enhance the ability for the customers to comply with GxP requirements. Finally, we review relevant Google Cloud certifications, attestations, and audits.

2.1 Electronic Records Requirements

The FDA, and its global counterparts, have developed regulations and procedures pertaining to the secure electronic storage of required documentation, including those related to regulatory submissions, internal compliance policies, supplier/purchasing information, and customer complaints, among other types. These provisions are intended to safeguard and prevent alteration or deletion of data that might compromise its integrity. In the U.S., compliance with the electronic records requirements is often referred to as "Part 11 Compliance", named after the CFR Part where the requirements can be found.[5] Google recognizes that these safeguards are in place to promote product safety and quality, and in this section we describe the processes and products that enable our customers to meet the security and integrity objectives advanced by Part 11 Compliance.

Table 1: Generalized GxP electronic record and signature requirements[6]

Electronic records requirements	Electronic signature requirements
• The ability to discern invalid or altered records • Secure, computer-generated, time-stamped audit trails • Protection of records to enable their accurate and ready retrieval • Authority checks for system access and use • Validation of systems to ensure accuracy, reliability, consistent performance • Operational system checks to enforce permitted event sequencing • Appropriate personnel qualifications including proper education, training, and experience • Appropriate controls over systems documentation including distribution, access, use and revision and change controls (audit trail of documentation development and modification) • Accountability policies for actions initiated under an individual's account	• At least two unique identification components (such as username & password) • Periodic checks, recalls, or revisions of authorization credentials • Use of transaction safeguards to prevent, detect, and report attempts at unauthorized use. • Controls for collaboration of two or more individuals that are not the genuine owner to use the individual's electronic signature • Loss management procedures to deauthorize potentially compromised tokens, cards, and other devices, and to issue temporary or permanent replacements with suitable controls. • Initial and periodic testing of devices, such as tokens or cards, to ensure proper functionality • Accountability policies for actions initiated under an individual's signature

[5] 21 CFR Part 11: Electronic Records: Electronic Signatures.

[6] Please note that while the entirety 21 CFR Part 11 technically remains in effect, FDA is currently exercising enforcement over certain requirements provided in these regulations. The agency has issued guidance that clarifies which requirements FDA is actively enforcing, a link to which can be found at FN 4. Life science customers should independently evaluate which requirements might apply to their record-keeping systems.

Behavioral requirements, such as restrictions on sharing passwords, training end users on the meaning of their electronic signature, and accountability for the use of an electronic signature are the responsibility of the customer, and are not further described in this section. Please refer to section 1 for more detail on the "Shared Responsibility Model."

Requirements related to the use of electronic records in GxP systems can be categorized into a few distinct subsets related to how such records are created, managed, and documented. Life science organizations utilizing electronic records systems should consider best practices around the topics of data retention, identity and access management, data security and audit trail, and data ownership, which we discuss below. We'll also briefly describe how Google meets GxP requirements on the backend functions we manage, and discuss some of the certifications that address Google Cloud's conformance to these standards.

Data Retention

GxP aligned document control and data storage systems should protect and retain records as well as enable their accurate and ready retrieval. In the past, when most records were kept in hardcopy form, organizations met retention requirements by maintaining documents at onsite or offsite physical storage facilities under predefined conditions that allowed for systematic retrieval. The term "ready retrieval" when applied to Cloud-based applications and storage could be understood to mean having robust backup and restore processes, and/or high availability systems. Storing data on the cloud can enable tailored retrieval of documentation at any point in its lifecycle, from multiple global locations simultaneously, with reliable data backup being an included benefit of using Google's platform versus other electronic record systems.

Google Cloud Object Lifecycle Management can be configured with lifecycle policies to create buckets of archival storage for data. For example, these storage buckets could be configured based on varying levels of access frequency. Older versions of existing documents that are less frequently accessed can be moved to more cost-effective Nearline or Coldline storage options, providing for much easier access overall in comparison to retrieving hardcopy documentation from an offsite storage facility.

Customers can also configure services such as BigQuery and Cloud Bigtable to automate expiration times for certain types of data, allowing each organization to configure expiration and deletion of documentation in line with their data retention policies. This eliminates the need for users to manually access and delete or preserve data that have required retention policies mandated by various regulations.

Identity & Access Management

GxP aligned systems require there to be controls in place that govern who has access rights to the data generally and/or on a periodic basis to help mitigate the risk of unauthorized alteration or deletion of records. Access rights should be established per the customer's segregation of duties policies, as well

as by job function or role, to ensure their organization's users can access everything they need within their role's responsibilities while limiting unauthorized access to critical or sensitive data.

Cloud Identity and Access Management (Cloud IAM) lets administrators authorize who can take action on specific resources, providing full control and visibility to manage cloud resources centrally. As Life Sciences organizations can have complex organizational structures and processes, as well as a global footprint, our suite of security and identity tools provides a unified view into the security policy across your entire organization with built-in auditing to ease compliance processes.

As contemplated in Part 11, electronic GxP systems should implement loss management procedures. Should a need arise to rotate account credentials, such as API keys, or encryption keys that protect sensitive health information, Google Cloud offers options to facilitate simple credential rotation in the Cloud IAM interface and rotation or destruction of asymmetric or symmetric encryption keys in Cloud Key Management Service.

GxP systems should also utilize appropriate digital signature standards, such as multi-factor authentication ("MFA"), to ensure record authenticity, integrity, and confidentiality. Google Cloud offers customers the ability to enable and require MFA, such as 2-step verification ("2SV"), for Cloud Identity accounts. Options for MFA include using security keys, push notifications to mobile devices, or one-time passwords.

Data Security and Audit Trail

Along with data retention requirements, GxP records should also be protected from unauthorized or unintentional alteration or deletion. Customers should ensure that they know when data was created, by whom, who has accessed that data, and if/when/how/and by whom changes were made. This can be accomplished through a robust and secure audit trail that captures the previous result, the changed result, the account that made the change, and an authoritative time and date stamp. This way the change in record is both attributable and detectable. Google Cloud has several solutions that accomplish this through tools like Cloud Audit Logs (which can create immutable logs for Admin Activity, Data Access, and System Events) and customizable monitoring and alerting capabilities.

For example, Cloud Logging allows you to store, search, analyze, monitor, and alert on log data and events from Google Cloud and other sources, including Amazon Web Services (AWS). We also offer strong encryption for data in transit on Google Cloud to guard against unauthorized access outside of our perimeter, and we are one of the only cloud service providers to offer encryption by default for data at rest. In addition, we enable customers to manage their own encryption keys for selected products through a key management service and provide healthcare-specific services for managing sensitive data like PHI and medical records.

Data Ownership

Google Cloud customers own their data, not Google. We do not access customer data for any reason other than those necessary to fulfill our contractual and legal obligations. Only a small group of Google employees, such as those who support authorized customer administrators, have access to customer data. Our employees' access rights and levels are based on their job function and role, using the concepts of least-privilege and need-to-know basis. Furthermore, given our commitment to transparency, we provide customers with the ability to view near real-time logs when Google administrators access customer content. Read our Trust Principles to learn more about Google Cloud's philosophy and commitments to customers.

Additionally, Google will retain, return, destroy, or delete personal data in accordance with the contract or service level agreements. We recommend that life sciences customers align their service level agreements with any data retention and/or regulatory requirements to retain data. To learn more about how data is deleted in Google Cloud, refer to the Data deletion on Google Cloud Platform whitepaper. Refer to our Data Security practices in our Cloud Data Processing Addendum for more information.

Physical Security

Google data centers feature a layered security model with custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics. The data center floor features laser beam intrusion detection. Only approved employees with specific roles may enter. Fewer than 1% of Google employees will ever step foot in one of our data centers. Where Google Cloud hosts servers in third-party data centers, we ensure Google-controlled physical security measures are implemented on top of the security layers provided by the data center operator. For more information, refer to the Google Infrastructure Security Design Overview.

Network Security

In addition to providing customers with data encryption in transit and at rest, Google Cloud also helps secure supporting systems and networks with products that define and enforce customer service perimeters, allowing for network segmentation, remote access, and Denial-of-Service defense. System administrators have the flexibility to securely scale and control how workloads connect regionally and globally, based on where their equipment and facilities are deployed. To support security of large networks of devices and equipment, Google has developed Application Layer Transport Security and Virtual Private Clouds with service controls that can help developers improve their design controls in accordance with FDA Quality System regulations, amongst others.

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. An important consideration for organizations as they introduce governance and control over network security policies is the adoption of Shared VPC networks. Network administrators must define routing and firewall rules at the host project level and provide explicit authorization for service project

resources to attach to individual subnets in the host project. This approach for allocating network access will enable organizations to require service project owners to meet certain security standards before being onboarded for production network access.

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. VPC Service Controls also dictate to which hosts outside the perimeter protected resources may connect or transfer data.

Application Security

Google Cloud provides a variety of application security products to protect and manage our customers' business applications with application testing, scanning, and API security features. Google recommends that all customers scan their workloads 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, which detects common injection flaws, the use of mixed HTTP/S content, and the use of insecure libraries within applications deployed on App Engine, Compute Engine, and Kubernetes Engine.

For end-to-end security across customers' API platforms, Google Cloud offers solutions such as Cloud Endpoints and Apigee. Either solution will enable developers to verify the identity of end users, using options such as JSON Web Tokens, API keys, or Oauth 2.0 tokens. While Cloud Endpoints is a solution specifically tailored for Google Cloud deployments, Apigee can be used in hybrid scenarios involving APIs deployed in Google Cloud and on premises. As part of the Apigee offering, Apigee Edge can protect backend systems from payload injection attacks (e.g. SQL injection) and detect and mask certain types of sensitive information (e.g. health information) before it is recorded in trace logs. Apigee Sense provides the ability to proactively defend APIs from threats or suspicious behavior.

Infrastructure Redundancy

Google designs the components of our platform to be highly redundant. This redundancy applies to our server design, data storage, network and Internet connectivity, and the software services themselves. This "redundancy of everything" includes the handling of errors by design and creates a solution that is not dependent on a single server, data center, or network connection. Google's data centers are geographically distributed to minimize the effects of regional disruptions on global products such as natural disasters and local outages. In the event of hardware, software, or network failure, platform services and control planes are automatically and instantly shifted from one facility to another so that platform services can continue without interruption. Google's highly redundant infrastructure also helps customers protect themselves from data loss. Google Cloud resources can be created and deployed across multiple regions and zones, allowing customers to build resilient and highly available systems.

For data storage at the physical level, Google stores customer data at rest in two types of systems: active storage systems and backup storage systems. While the active storage systems are Google Cloud's production servers running Google's application and storage layers, our backup storage

systems house full and incremental copies of the active systems for a defined period of time to help Google recover data and systems in the event of a catastrophic outage or disaster. Throughout the storage systems described above, Customer data is encrypted when stored at rest. Encryption of data at rest occurs at the application and storage layers, on both active and backup storage media. The details of Google's encryption techniques are discussed in greater detail in Google's Cloud Security whitepaper.

2.2 Relevant GxP Product Features: Validation and Infrastructure Qualification

Infrastructure Qualification

One of the core needs for GxP computerized systems is that they be *validated* to ensure the system meets user requirements.[7] In a traditional hosted environment, the first step to building a validated computerized system is *qualifying* the infrastructure.[8] Similar to qualifying 'on prem' infrastructure, a customer would follow their infrastructure qualification process to document the technical specifications required, build the cloud-based infrastructure to those components, and then verify that the actual build meets the specifications. The customer's validation methodology should outline the specific documentation requirements, and the build documentation produced during this process could be used to support the infrastructure's qualified state.

Cloud resources, such as Compute Engine or Cloud Storage, can be provisioned through the Google Cloud Console or programmatically via Cloud Deployment Manager, Hashicorp Terraform, or directly via GCP's RESTful APIs. Cloud Deployment Manager is an infrastructure deployment service that automates the creation and management of Google Cloud resources. It enables customers to write flexible template and configuration files and use them to create deployments that have a variety of Cloud Platform services, such as Cloud Storage, Compute Engine, and Cloud SQL, configured to work together. With Deployment Manager a customer can view the Manifest, which contains all of the inputs, specifications, upload files, etc. (the "requirements") and a report of the actual build, which can be used to show that the cloud resources have been qualified. Then the customer can proceed with any application validation activities.

Change Management and Operational Monitoring

In addition to validating the system infrastructure, GxP aligned systems should also implement appropriate change control procedures regarding infrastructure and application components. This can

[7] NIST defines validation as: "Confirmation, through the provision of objective evidence, that the requirements for a specific intended use or application have been fulfilled." (*see* NIST SP 800-160 [Superseded] (ISO 9000)).
[8] NIST defines qualifying as: "Process of demonstrating whether an entity is capable of fulfilling specified requirements." (*see* NIST SP 800-160 [Superseded] (ISO/IEC/IEEE 12207:2017)). Retrieved from https://csrc.nist.gov/Glossary/Term/qualification

be achieved by ensuring that only authorized changes are made to systems, only authorized users have the ability to make changes, and through ongoing monitoring to ensure that there are no operational issues or security concerns. Customers should incorporate their unique change management process controls into the Google Cloud ecosystem to evaluate the impact of any changes made to the cloud infrastructure, application configurations, or changes to data within applications.

An organization should also establish guardrails in the form of policy constraints specifying which teams need to have access to what types of data, as well as what restrictions apply to that access. For example, customers can ensure that teams are only utilizing approved images for virtual machine use.

Customers can use Security Command Center (CSCC) to view and monitor an inventory of their cloud assets, review access rights to their resources, receive alerts on policy violations from Forseti (e.g. overly permissive Cloud Storage ACLs or Compute Engine firewall rules), and detect common web vulnerabilities, all from a single, centralized dashboard. Our customers can also control who has access to make changes to their infrastructure through Cloud IAM, allowing them to implement change control policies and admin review workflows. After the approved Google Cloud infrastructure change is made, it is recommended that users perform a targeted verification activity to confirm the change had the expected results.

Changes to server configurations, including any changes to the specifications, can be controlled through the Cloud Console or Cloud Deployment Manager, and supporting documentation from Deployment Manager can be used to show that the changes were made per the requirements. The Cloud Console represents the central user interface for a customer to manage, create, edit, or view activity related to Google Cloud resources. Additionally, customers can use the Cloud SDK or Cloud Shell, which enables Google Cloud customers to manage infrastructure and applications from the command line in any browser.

At Google Cloud, we constantly monitor for malicious activity, handle security incidents, and support operational processes that prevent, detect, and respond to threats and performance issues. In addition, The Google Cloud operations suite aggregates metrics, logs, and events from infrastructure, giving customers the ability to proactively monitor and resolve any performance issues in a controlled manner. The operations suite also maintains the change history for the server itself in the form of the audit trail, which can be used to show that all changes have been authorized and followed appropriate change control procedures. Cloud Logging enables customers to search, store, analyze, monitor and be alerted to any changes or updates in log data.

Detailed documentation on the Google Cloud products and operational processes is available to customers on our Google Cloud Products page.

Incident Response

Effective incident response is not only key to managing and recovering from incidents but also for preventing future ones. Google Cloud's comprehensive incident response capabilities leverage the combination of dedicated experts, efficient processes, and sophisticated monitoring to proactively detect incidents, contain them, mitigate impact, inform customers, and reconstitute services in a trusted manner. Here is a high-level view of the incident management response process broken down by phases:

1. **Identification.** Early and accurate identification of incidents is key to strong and effective incident management. The focus of this phase is to monitor security events to detect and report on potential data incidents.
2. **Coordination.** When an incident is reported, the oncall responder reviews and evaluates the nature of the incident report to determine if it represents a potential data incident, and initiates Google's Incident Response Process.
3. **Resolution.** At this stage we focus on investigating the root cause, limiting the impact of the incident, resolving immediate security risks (if any), implementing necessary fixes as part of remediation, and recovering affected systems, data, and services.
4. **Continuous improvement.** We analyze each incident to gain new insights that help us enhance our tools, trainings and processes, as well as Google's overall security and privacy data protection program

To learn more about our incident management, please read our Data Incident Response whitepaper.

2.3 Satisfying GxP Requirements

Regulated life science organizations, including pharmaceutical, medical device, and biological product manufacturers that operate in the US or in other global healthcare markets dedicate significant resources to developing, managing, and operating GxP systems. In particular, valuable time and effort are expended developing systems and protocols designed to comply with Current Good Manufacturing Practice (GMP) and Quality System (QS) regulations.[9] In the US, GMP/QS requirements are enforced by the FDA, and require life science organizations to establish procedures to ensure the proper design, monitoring and control of manufacturing processes and facilities. Though organizations are granted a certain amount of discretion regarding the specifics of their systems, compliant GMP/QS systems must broadly address development and production topics that could impact the safety and effectiveness of manufactured products. Such topics include:

[9] FDA's Current Good Manufacturing Practice regulations applicable to pharmaceutical products can be found at 21 CFR Parts 210 & 211; and the Quality System requirements applicable to medical devices are provided at 21 CFR Part 820.

- Management responsibility;
- Personnel training;
- Records and reports;
- Quality Audits;
- Purchasing controls; and
- Supplier evaluations

These systems often involve substantial recordkeeping obligations, and organizations are required to ensure that their documentation, data management, and change control processes are compliant. Below we cover some ways that customers can streamline their compliance initiatives and build reliability into these electronic systems by switching to cloud-based applications.

Management Responsibilities:

Typically, GxP systems require that life science organizations establish and maintain official policy and objectives for ensuring product quality.[10] Management with executive responsibility is required to ensure that the quality policy is understood, implemented, and maintained at all levels of the organization. Part of this responsibility is to allocate authority to appropriate personnel who manage, perform, and assess work affecting quality. In a cloud-based IT environment, this will include setting permissions and access authority to the proper personnel, and overseeing and managing staff regarding their access to, and use of, certain electronic GxP systems.

Customers using Google Cloud can configure Cloud IAM permissions to control access to their cloud resources and limit access by their own administrators, curating the right amount of access at the project, folder or dataset level. This includes an extensive list of permissions and the predefined roles that grant them. You can also create your own custom roles that contain exactly the permissions you specify.

To help mitigate risks such as the misconfiguration of employee access controls or attackers taking advantage of compromised accounts, VPC Service Controls enables customers to define a security perimeter around Google Cloud resources, such as Cloud Storage, BigQuery, or Bigtable to prevent data exfiltration. Identity-Aware Proxy (IAP) enables customers to control access to cloud applications and VMs based on the user's identity and the context of their request. Customers can also control who has access to your Cloud Storage buckets and objects as well as the level of access. For more information, refer to the documentation page for Cloud Storage.

[10] See 21 CFR Part 211, Subpart B—Organization and Personnel; 21 CFR 820 Part 820, Subpart B—Quality System Requirements.

Organization and Personnel Training:

Life science organizations are responsible for developing and implementing their company's quality policies, and maintaining adequate organizational structure to ensure that their products are designed and produced in accordance with regulatory requirements.[11] These responsibilities include ensuring personnel have the necessary background, training, and experience to correctly perform all assigned quality-related activities. When those functions include the use of Google Cloud services to configure infrastructure support of electronic GxP systems, experience with Google Cloud services should be taken into consideration when hiring and/or training personnel. Customers can leverage a number of Google Cloud trainings to provide additional skills and knowledge to entire teams in areas such as architecting with Google Kubernetes Engine and using machine learning with TensorFlow on Google Cloud. Your personnel will be able to obtain certifications that demonstrate their technical skills in a particular technology or job role.

Customers should also consider updating their policies and procedures and/or any other organizational documents that cover personnel education and experience requirements as well as training curricula management. We encourage our customers to get acquainted with our Google Cloud Customer Responsibility Matrix.

Records and Reports:

A central element of both the GMP and QS regulations is the requirement to establish records systems that can be easily accessed and reviewed during agency inspection. The purpose of these systems is to ensure product quality procedures are adequately maintained and followed.[12] For example, records of each significant step of the distribution process, including the manufacture, processing, packing, and holding of a particular product or batch of product is usually required. In addition, regulated organizations must establish procedures for receiving, reviewing, and evaluating customer complaints, and maintain comprehensive records detailing how each received complaint was resolved. For purposes of regulatory agency inspection, proper record management that ensures the integrity of data is critical.

As mentioned earlier, Google Cloud offers customers tools like Cloud Audit Logs that help security teams maintain audit trails in Google Cloud and view detailed information about Admin activity, data access, and system events. Cloud Audit Logs reside in highly protected storage, resulting in a secure, immutable, and highly durable audit trail. Customers can also use Cloud Logging to store, search, analyze, monitor, and alert on log data and events from Google Cloud. Our API also allows ingestion of any custom log data from any source and can be combined with Google Cloud's data and analytics products for advanced log analysis.

More information on Google Cloud's operation suite is available on our Operations product page and documentation pages.

---

[11] Id.
[12] See 21 CFR Part 211, Subpart J--Records and Reports; 21 CFR Part 820, Subpart M--Records.

Quality Audits:

GxP-compliant life science organizations are required to establish procedures for conducting quality audits. Such audits are undertaken to ensure that the company's quality systems are in compliance with GxP regulations and to determine their overall effectiveness.[13] As part of this process, organizations must generate and maintain reports of the results of each quality audit, and such reports should be reviewed by responsible management to determine whether corrective actions are necessary. Regulatory inspectors will often ask to see documentation that quality audits are being conducted.

Customers conducting quality audits of their systems can take advantage of Google Cloud services to assist with the audit process. By leveraging services like Google Cloud's operations suite, Cloud IAM, and open source tools like Forseti Security, you can maintain a comprehensive view and history of what is going on in your Google Cloud environment without much impact of your existing quality audit processes.

Purchasing Controls:

As part of their GxP controls, manufacturers of life science products are responsible for ensuring that all purchased or otherwise received products conform to specified requirements.[14] Based on the size and complexity of the organization, life science organizations often have different needs and expectations related to their IT infrastructure. However, in every case, regulated organizations must maintain records that clearly describe established specification requirements along with other purchasing control documentation. With Google Cloud, customers can view our reports and certifications that represent independent verification of our controls.

Supplier Evaluations:

Organizations with GxP obligations are responsible for evaluating and selecting potential suppliers, contractors, and consultants on the basis of their ability to meet specified requirements, including those related to product quality.[15] As part of this process, company management must define the type and extent of control to be exercised over the product, services, and suppliers based on the evaluation results. Further, documentation of this process may be requested by the FDA or other regulatory bodies as part of a compliance inspection. Thus, establishing and maintaining records of evaluated and acceptable suppliers, contractors, and consultants is critical for life science organizations.

---

[13] See 21 CFR § 820.22.
[14] See 21 CFR Part 820, Subpart E--Purchasing Controls.
[15] Id.

Our customers and regulators expect independent verification of security, privacy, and compliance controls. Google undergoes several independent third-party audits on a regular basis to provide this assurance. Some of the key international standards we are audited against are:

- ISO/IEC 27001 (Information Security Management)
- ISO/IEC 27017 (Cloud Security)
- ISO/IEC 27018 (Cloud Privacy)
- SOC 2 and SOC 3 reports

Google also participates in sector and country-specific frameworks, such as FedRAMP (US government), HITRUST CSF (primarily Healthcare), BSI C5 (Germany), MTCS (Singapore), and many others. We also provide resource documents and mappings to frameworks and laws where formal certifications or attestations may not be required or applied. For a complete listing of our compliance offerings, please visit our Compliance resource center.

2.4 Applicable Google Cloud Certifications, Attestations, & Audits

To help life sciences customers with compliance and reporting, we share information, best practices, and easy access to documentation. Our products regularly undergo independent verification of security, privacy, and compliance controls, achieving certifications against a number of standards. Certifications and attestations related to information security (e.g. ISO 27000 series, CSA STAR), as well as some of the specific healthcare related certifications, regulations, and frameworks (e.g. HITRUST, FedRAMP, HIPAA), help support our regulated customers' needs. Additionally, many of the controls tested in our SOC reports, especially related to security, user access, change management, and deployment procedures give customers transparency to the design and operating effectiveness of specific controls relevant to supporting GxP requirements.

To see our full list of applicable certifications and to learn more, refer to our Standards, Regulations, and Certifications page.

2.5 Information Google Cloud May Provide for Use if Required in an FDA Regulatory Submission

Google Cloud provides extensive publicly-available documentation of our procedures, practices, and security measures that may be useful in regulatory submissions to demonstrate the safety and effectiveness of a Google Cloud-integrated medical device or to illustrate how Google Cloud supports a quality system. Much of this documentation has been linked throughout this whitepaper.

In addition, Google Cloud customers may be provided more detailed documentation about the products and services they use. Some documentation may be confidential and/or protected by non-disclosure agreements between Google Cloud and our customers. In the event protected information is necessary

for inclusion in an FDA regulatory submission, and its inclusion is agreed upon in advance by Google Cloud, it should be marked as confidential to indicate to FDA that the information should not be released under the Freedom of Information Act and FDA's information disclosure regulations at 21 CFR Part 20. If the FDA requires additional non-public documentation for purposes of reviewing a regulatory submission, the potential release to the FDA of such information should be discussed in individual contractual agreements.

2.6 Additional Healthcare Compliance Support

Google Cloud maintains an active, ongoing repository of information, best practices, and documentation related to healthcare and life science compliance and reporting for various regions around the world. We also highlight some of those key healthcare issues below.

HIPAA Compliance

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a US federal law that established data privacy and security requirements for certain entities and individuals aimed at safeguarding individuals' health information. HIPAA mandates privacy and security protections for protected health information (PHI) and applies to individuals and entities that meet the definition of "covered entities" or "business associates" under HIPAA. Customers who are subject to HIPAA and want to utilize any Google Cloud products in connection with PHI must review and accept Google's Business Associate Agreement (BAA). While the U.S. Department of Health & Human Services (HHS) does not recognize a formal certification process for HIPAA compliance, Google Cloud regularly undergoes several independent audits to assess the security, privacy, operational, and compliance controls we have in place based on global standards that encompass requirements outlined in HIPAA. HIPAA compliance is a shared responsibility between our customers and us. To learn more, refer to our HIPAA Compliance Guide for GCP.

3.0 Conclusion

Life science organizations can take advantage of Google Cloud products and services to streamline product development, execute and track quality manufacturing processes, and enable a robust software development lifecycle as part of compliance with FDA and other global regulatory requirements. Through significant investment in the quality and security of our services, we have made it easier for life science customers to demonstrate compliance with regulatory requirements. In securing our systems and protecting them against threats, we enable software developers to benefit from our technologies and practices while mitigating risk to patients and users of their products.

4.0 Appendices

For reference, we have included lists of Google Cloud products that may help life sciences customers and healthcare organizations with regulatory compliance, including Google Cloud security-related whitepapers and resources, as well as applicable regulations, guidance, and standards for life sciences products.

4.1 Google Whitepapers and Resources related to Security

- Google Security Whitepaper
- Google Infrastructure Security Design Overview
- Encryption at Rest in Google Cloud Platform
- Encryption in Transit in Google Cloud
- Application Layer Transport Security in Google Cloud
- Google Cloud's Approach to Security (ebook)
- HIPAA Compliance Guide for GCP

4.2 Relevant Regulations and Guidance for GxP Manufacturers

Title	Summary
Quality Management Systems (ISO 9001:2000)	This international standard specifies the requirements for a quality management system where an organization needs to demonstrate its ability to consistently provide product that meets customer and applicable regulatory requirements, and aims to enhance customer satisfaction through the effective application of the system, including processes for continual improvement of the system and the assurance of conformity to customer and applicable regulatory requirements.
Quality System Regulation (21 CFR Part 820)	This US regulatory part requires that each manufacturer shall establish and maintain a quality system that is appropriate for the specific medical device(s) designed or manufactured, and that meets the requirements of this part.
Q10 Pharmaceutical Quality System Guidance (ICH Q10)	This internationally harmonized guidance is intended to assist pharmaceutical manufacturers by describing a model for an effective quality management system for the pharmaceutical industry, referred to as the pharmaceutical quality system.

Current Good Manufacturing Practice (CGMP) in Manufacturing, Processing, Packing, or Holding of Drugs; General (21 CFR Part 210)	This US regulatory part introduces the minimum practices and methods to be used in, and the facilities or controls to be used for the manufacture, processing, packing, or holding of a drug to assure safety, identity, and strength as well as meets the quality and purity characteristics that it purports or is represented to have.
Current Good Manufacturing Practice (CGMP) for Finished Pharmaceuticals (21 CFR Part 211)	This US regulatory part describes the minimum current good manufacturing practices for production of human and animal drug products. The controls outlined include those for: • Organization and personnel; • Buildings and facilities; • Equipment; • Components, containers, and closures; • Production and processes; • Packaging and labeling; • Product and materials holding and distribution; • Sampling and testing; • Record and report management; and • Returned and salvaged products.
Electronic Records and Electronic Signatures (21 CFR Part 11)	The FDA provides criteria and controls for electronic records, electronic signatures, and handwritten signatures executed to electronic records in order to establish a trustworthy, reliable, and generally equivalent alternative to paper records and handwritten signatures on paper documents. This part also describes controls for open systems in which system access is not controlled by those responsible for the content, and closed systems in which access is controlled by those responsible for content. The latter set of controls are those applicable for life sciences customers of GCP.
FDA Guidance for Industry: Part 11, Electronic Records; Electronic Signatures — Scope and Application Update December 2018	This FDA guidance on the scope and application of regulatory requirements for electronic records and electronic signatures provides GxP manufacturers with more detail on the agency's approach. The FDA clarifies that computer systems used to generate paper records do not have additional requirements as long as the paper records themselves are compliant. In addition, the agency provides detail on its intention to exercise enforcement discretion for computer system validation, computer-generated audit trails, legacy systems, record copies, and record retention.

5.0 Additional Resources

As you continue on your journey to build GxP aligned devices, equipment, systems or applications, we invite you to take advantage of the resources listed below.

Learn More

	Google Cloud	G Suite
Learn Why Other Organizations are Choosing Google Cloud	Why Google Cloud?	Why G Suite
Learn More About Our Services	Google Cloud Solutions	G Suite Learning Center
Learn More About Our Pricing	Google Cloud Pricing	G Suite Solution

Engage

	Google Cloud	G Suite
Try Google Cloud For Free	GCP Free Tier	G Suite Free Trial
Call Our Knowledge Center	844-613-7589	855-312-7191
Have Questions Regarding Security, Privacy or Compliance?	Contact our experts at compliance@google.com	

Act

	Google Cloud	G Suite
Get Google On Your Team	Fill out this form or call 844-613-7589	Fill out this form or call 855-312-7191
Train Your Team	Google Cloud Training	G Suite Training
Quickstarts - *Deploy your first solution in 10 minutes or less*	Getting Started With GCP	G Suite Quick Start Guide

Get Support

	Google Cloud	G Suite
Frequently Asked Questions	GCP FAQs	G Suite FAQs
Customer Technical Support	Contact our Google Cloud Support Center	