Google Cloud

Safeguarding Health Data: Preserving Privacy in the Digital Age with Google Cloud

aiforia®

AI for image analysis

Introduction

As more healthcare and life sciences organizations adopt cloud-based resources, huge amounts of data are being stored, processed, and analyzed across platforms. At Google Cloud, the privacy and security of customer data are primary design criteria that underpin all the services that we offer. Given the sensitive nature of individually-identifiable health information and other types of personally identifiable information (PII), the protection of healthcare data and the systems it resides on is of critical importance. While we help with support for regulations like the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the General Data Protection Regulation (GDPR), we also understand that at the core, customers want assurances around how we use, process, and handle customer data.

As the use of electronic health records (EHR) continues to rise, government agencies and healthcare providers need digital assurances that health information is protected and complies with key regulations such as HIPAA. They also need to ensure that any sensitive data can be protected–no matter the scale and speed at which they operate.

Security is a priority at Google

Robust infrastructure

Google's global infrastructure benefits from massive investments in security, providing a strong foundation for protecting healthcare data.

Strong compliance framework

Google Cloud is HIPAA compliant and offers support for other global regulations like GDPR.

Trust through transparency

Access Transparency provides visibility into our actions.
Perform regular audits of access by administrators.
Google Cloud Trust Principles.

AI and ML for security

Leveraging AI and ML, Google Cloud offers advanced threat detection and response capabilities.

Dedicated healthcare focus

With its Healthcare API and other offerings, Google Cloud demonstrates a clear commitment to the healthcare industry and its specific security needs.

Advanced Data Protection Tools

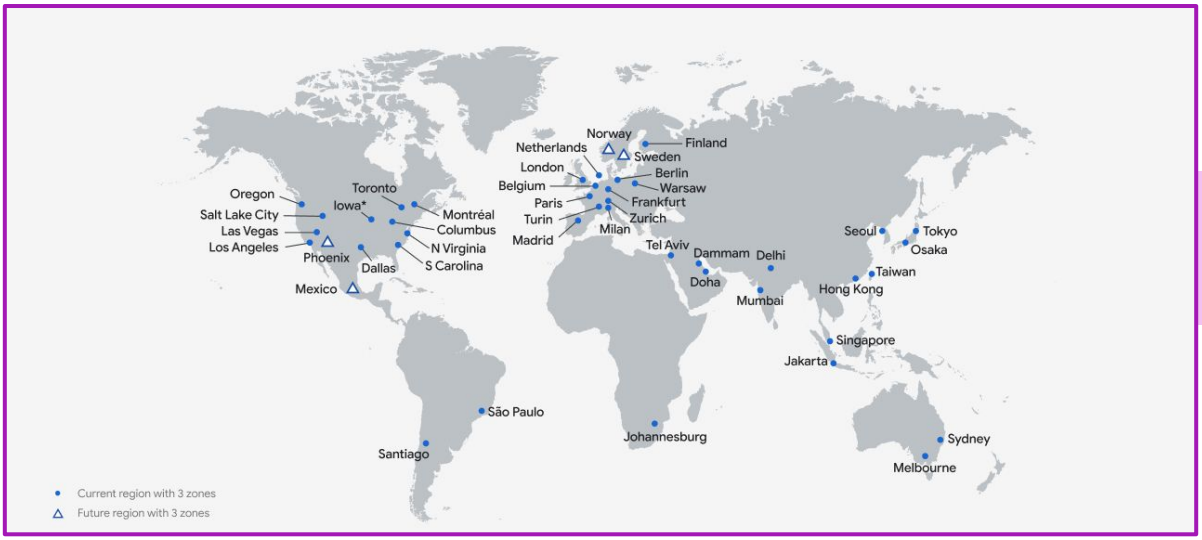
Cloud Data Loss Prevention (DLP):
Detects, classifies, and protects sensitive data across cloud, on-premises, and hybrid environments.

Healthcare De-ID:
Protects patient privacy by removing or masking personally identifiable information (PII).

To be truly global we need to be local

We invest at scale to increase our presence in many places around the world. Our investment in technical infrastructure locally provides the gateway for customers to take advantage of Google's Transformational Cloud Platform offering adjusted to their local needs.

40
Regions
121
Zones
187
Network edge locations
200+
Countries and territories



Smarter

The data cloud

- Embrace the **full data lifecycle** to improve decision making
- **Democratize access** to all data to drive business outcomes at any scale
- **Leading AI solutions** helps businesses predict and automate

Freedom

The open cloud

- Harness the **flexibility of open source** innovation throughout the industry
- Enjoy the **freedom of a multi cloud environment** to build and run apps anywhere
- **Leverage solutions from our partner ecosystem** to expand your technology choices

The collaboration cloud

Connections

- **Reimagined work environment**
- New ways to strengthen **human connections**
- Help companies **connect with customers and partners**

The trusted cloud

Protection

- **A secure platform** that delivers transparency and enables sovereignty
- A proven **zero-trust architecture**
- **Shared fate,** not shared responsibility

Google Cloud regions provide our customers with best in class infrastructure to support their business

Speed

Serve your local end users with a low-latency, fast experience.

Availability

Reduce downtime and increase resilience against disasters.

Sustainability

Reduce the carbon footprint of your organization and hit Environmental Social and Governance (ECG) targets.

Trust

Secure infrastructure, in the country allowing for advanced sovereignty controls: data residency, cryptography, transparency, survivability.

Trusted Cloud - Shared Fate

It is our commitment to be **active partners** as our customers deploy securely on our platform, not delineators of where our responsibility ends. **We stand with our customers from day one**, helping them implement best practices for safely migrating to and operating in our **Trusted Cloud**.

Security by design

- Multiple levels of encryption plus physical and logical security
- Google-built hardware optimized for security
- Comprehensive security throughout the stack
- Rigorous controls of our software supply chain and binary authorization
- Security testing, red-teaming, threat analysis, and vulnerability research
- Open-source initiatives championed

Security by default

- Continuously updated security defaults
- Security blueprints and landing zones
- Embedded default security configurations
- Default encryption at rest

Security in deployment

- Security built on experience
- Tools and monitoring
- Data encryption
- Advanced security features

Customers own their data, not Google; therefore, you decide how your data will be used on Google Cloud. At Google Cloud, we commit to **never using your data for any purpose other than those necessary** to fulfill our contractual and legal obligations. To truly embrace Shared Fate, you need confidence that you can still **retain a level of independence and control over infrastructure** and operations that you don't own. This thinking is at the root of global mandates for **Digital Sovereignty**. So, Google Cloud is committed to **providing our customers with flexible sovereignty solutions on their terms** to help meet current and emerging requirements.

Google's vision of sovereignty is not only about data protection.

Data Sovereignty

You keep all control over encryption and access to your data.

Operational Sovereignty

You have visibility and control over provider operations.

Software Sovereignty

You can run workloads without dependence on provider's software.

Security products supporting a safe cloud journey

At the core of a **zero trust approach** is the idea that implicit trust in any single component of a complex, interconnected system can create significant security risks. Instead, **trust needs to be established via multiple mechanisms and continuously verified.** Embarking on a zero trust architecture journey gives modern security practitioners defense in depth, with the ability to methodically shut down attack vectors. Our extensive range of security products represents a rich heritage of Google security that your business can benefit from.

Google SecOps

Empowers security teams to better defend against today's and tomorrow's threats.

VirusTotal

Analyzes suspicious files, domains, IPs, and URLs to detect malware.

BeyondCorp Enterprise

Secures internet and application access from anywhere.

Cloud Intrusion Detection System

Detects network-based threats with industry leading security.

Security Command Center

Manages security vulnerabilities and threats from one platform.

reCAPTCHA

Protects third-party websites and collects human-labeled data for machine learning.

Cloud Armor

Provides a managed Distributed Denial of Service (DDoS) protection service.

Cloud Data Loss Prevention

Helps discover, classify, and protect sensitive data.

Chrome Browser

The most used and secure browser for the modern-day challenge of the security landscape.

Chrome OS

Linux-based operating system derived from open-source Chromium OS.

Google Cloud's compliance offerings for security

To help you 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 global standards to earn your trust. We're constantly working to expand our coverage.

- ISO/IEC 27001
- ISO/IEC 27017
- ISO/IEC 27110
- SNI 27001

- ISO 22301:2019
- BS EN ISO 22301:2019

- SOC 2
- SOC 3

- 2G3M (Japan)
- NEN (Netherlands)

- (C5:2020)

- Center for Internet Security (CIS) Benchmarks
- K-ISMS (Korea)

- Class C license (Kingdom of Saudi Arabia)

- EU Standard Contractual Clauses

- BSI Critical Infrastructure (KRITIS)

- Qatar National Information Assurance (NIA)

Customer success stories

Mayo Clinic transforms the future of healthcare with Google Cloud

Mayo Clinic has chosen to partner with Google to positively transform patient and clinician experiences, improve diagnostics and patient outcomes, as well as enable it to conduct unparalleled clinical research.

MAYO CLINIC

Google Cloud results:

- Create machine learning models for serious and complex diseases.
- Enable Mayo Clinic to lay out a roadmap of cloud and AI-enabled solutions.
- Help develop a bold, new digital strategy to advance the diagnosis and treatment of disease.
- Focus on revolutionizing healthcare delivery by leveraging innovative cloud technology, industry leading AI, and specific healthcare solutions.

> With Google Cloud's secure and compliant digital platform, we will be able to leverage innovative cloud technology, industry leading AI and healthcare specific solutions, so we can focus on revolutionizing healthcare delivery and taking care of our patients."
> —**Christopher Ross Chief Information Officer, Mayo Clinic**

AZ Delta: Bringing personalized medicine one step closer with data analytics

AZ Delta has built a comprehensive medical data analytics platform that generates unprecedented insight without compromising security supported by Google Cloud.

azdelta
Uw ziekenhuis.

Google Cloud results:

- Keeps sensitive medical data secure with Virtual Private Cloud and three-factor authentication with Cloud Identity.
- Collates and analyzes hundreds of millions of data points at speed for greater insight with BigQuery.
- Engages machine learning tools to help physicians plan the optimal treatment pathways for their patient's unique needs.
- Cuts data query run time from 15 minutes to 15 seconds.

> "I knew that Google Cloud was powerful enough to build the data platform we envisioned. And it also combined ease of use with comprehensive security options for our most sensitive data. It was the only infrastructure that we looked at that fulfilled all our criteria."
> —**Peter De Jaeger, Chief Innovation Officer, AZ Delta**

Google Cloud

aiforia®
AI for image analysis

Thank you!