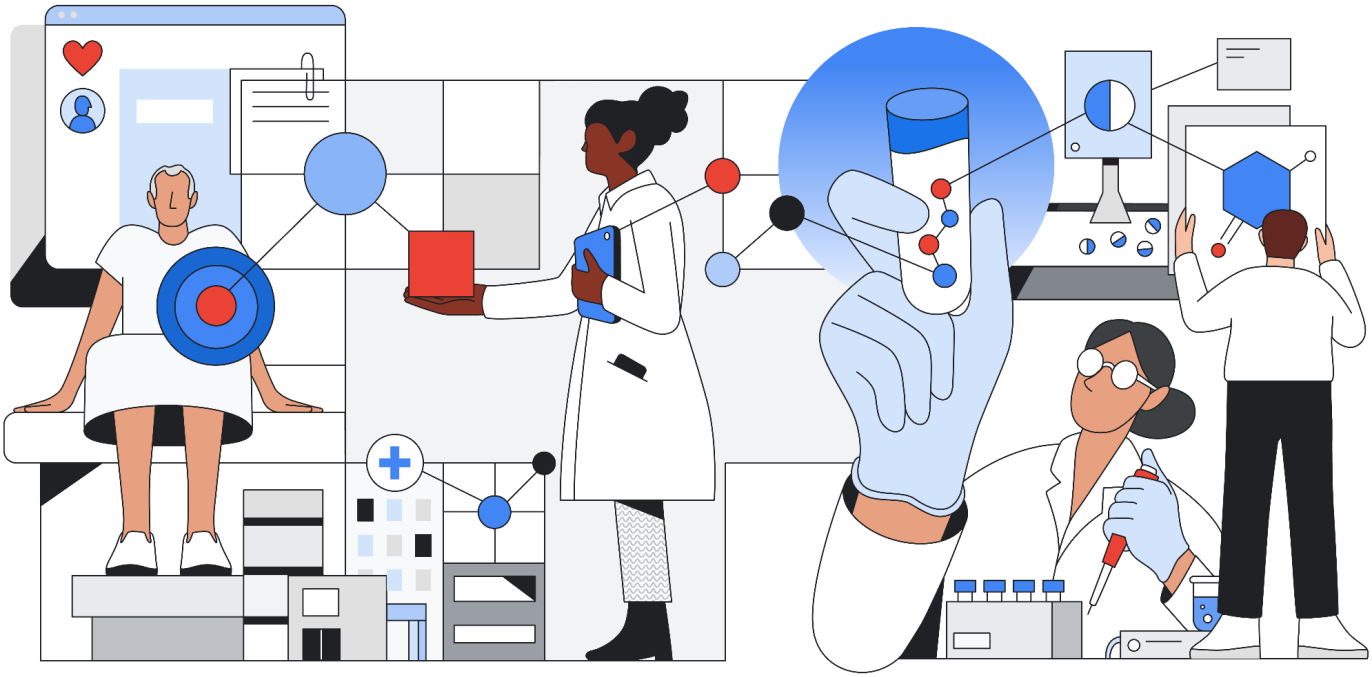
Google Cloud

Google Cloud Whitepaper
June 2023

Insights into the German Healthcare Industry



Disclaimer

The content contained herein is correct as of June 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.

Introduction

The Healthcare and Life Sciences (HCLS) industry in Germany has experienced a shift in momentum in recent years as new regulations increasingly emphasize digital transformation. Historically, a number of regulators have outlined the requirements for securing different parts of Germany's digital infrastructure. The recent evolution of the industry includes the Bundestag's 2019 passing of the Digital Healthcare Act (DVG). DVG introduced a dedicated path for digitally accessible patient data and interactions – expanding the connection of infrastructure, healthcare facilities, practitioner, and patients. While German HCLS organizations have previously ranked lower in digital adoption, recent trends have indicated an emphasis on increased adoption driven by the DVG.[1]

With more organizations focused on digital transformation and transitioning to storing their data in the cloud, there is an increasing need to address important industry regulations, including the protection of user data. Notably, this scenario increases in complexity when different regulations cover similar control areas and organizations must navigate the complexity of ensuring they are compliant with all applicable regulations. HCLS organizations can have different, sometimes overlapping use cases across business units, which can lead to organizations needing additional assurances that they have met all of the standards set by each regulatory entity.

Consequently, German HCLS organizations are looking to partner with organizations who can help them achieve digital transformation while ensuring security, privacy, reliability, and scalability - all while helping them meet their customer and regulatory requirements. Google Cloud recognizes that the challenge lies in ensuring that technology risks are managed, regulatory compliance is addressed, while patient, customer, and other stakeholder outcomes are maintained or improved. In this paper, we'll explore German healthcare trends, key regulations, and how Google Cloud is helping German HCLS customers meet this industry shift.

General German Healthcare Trends

Shifting to digital records

As the digital ecosystem has evolved, regulations have shifted to requiring healthcare organizations to store their data digitally to enable patients easier access. In practice, this means pharmaceutical companies, hospitals, and other applicable entities are required to utilize an electronic patient record.

Consumer reception is mixed

The move to digital records impacts consumers who shift from paper to digital. Like many infrastructural changes, they take time. While 90% of general practitioners in Germany are now

[1] Bertelsmann Digital Health Index

connected to the digital healthcare system (Telematikinfrastruktur), 95% of communication between physicians and hospitals remains paper-based.[2] To advance the shift from paper to digital healthcare platforms, enhanced regulator, practitioner, and patient alignment and trust is needed. Regulators have developed policies and control requirements for the secure development of healthcare platforms for organizations to maintain to ensure their platforms are designed and developed securely and meet the applicable regulations.

German HCLS Regulations

German regulations typically fall into three major buckets:

1. Regulations that come from the Sozialgesetzbuch
2. Regulations that are created by the German Federal Office for Information Security
3. The Bundesdatenschutzgesetz - an expansion of the EU's General Data Protection Regulation (GDPR)

Figure 1: German Regulatory Landscape Overview

The list below represents critical regulations within Germany that include references to security requirements.

[2] Messal, H., Müller, T., Richter, L., & Silberzahn, T. (2022, March 16). Germany's e-health transformation makes uneven progress. McKinsey; https://www.mckinsey.com/industries/life-sciences/our-insights/germanys-ehealth-transformation-makes-good-but-uneven-progress

Sozialgesetzbuch (SGB) - Social Code

The Sozialgesetzbuch (SGB) is a large overarching set of regulations regarding "social" laws. Specifically, Book V and X define "Social Data" as any information regarding an identified person or which can be used to identify a person. They outline general requirements for how Social Data must be stored and collected. Because the vast majority of healthcare data falls under the broader umbrella of Social Data, it must be treated as sensitive and falls under the requirements outlined in the SGB.

Gematik - German Healthcare System Digital Provider

Gematik is an organization tasked with defining the specific requirements around protecting Germany's Critical Infrastructure as outlined in the SGB. Specifically, Gematik's regulations contain a collection of objectives, controls, and technical requirements for securing Germany's entire digital healthcare system (Telematikinfrastruktur). While there are thousands of requirements within Gematik's regulations, the significant requirements center around data protection and security requirements. The controls include:

- Stipulations around how and where data can be transmitted.
- The high availability of data.
- The interoperability of the centralized Telematikinfrastruktur and external infrastructure.

Patientendaten-Schutz-Gesetz (PDSG) - Patient Data Protection Act

The Patient Data Protection Act (PDSG) provides more specific required security controls around Social Data and clarifies the responsibility of data protection within the healthcare industry. Service providers are responsible for the authentication and transmission of data from their infrastructure to the Telematik centralized infrastructure. They must adequately commission, maintain, and securely use these components. For example, Telematik connectors must be secured against unauthorized access and use state-of-the-art encryption methods to ensure the secure transfer of the data into the centralized infrastructure.

Digitale-Versorgung-Gesetz (DVG) - Digital Healthcare Act

The Digital Healthcare Act is a regulatory framework adopted by Germany's parliament in late 2019. With its passing, DVG introduced "prescription app" as part of patient healthcare. Those insured on statutory health insurance are now entitled to healthcare through digital health applications Digitale Gesundheitsanwendungen (DiGA). Applications can be prescribed by physicians for patients to use as part of their healthcare and are reimbursed by health insurers.

Digitale-Gesundheitsanwendungen-Verordnung (DiGAV) - Digital Health Applications Ordinance

The Digital Health Applications Ordinance (DiGAV), an ordinance that applies to all digital health applications in Germany, describes how manufacturers can demonstrate that their digital technologies meet the legal requirements of the DVG. DiGAV contains a number of checklists related to interoperability and portability, information security, and quality assurance. Among the critical requirements of the DiGAV include limitations on the location of data processing, adherence to open source technologies emphasizing highly interoperable services, and conformity to internationally observed quality standards.

German Federal Office for Information Security (BSI)

The German Federal Office for Information Security (BSI) specifies in various Technische Richtlinien (TRs) the specifics of the secure handling of information in healthcare.

Technische Richtlinien (TR) - Technical Regulations

These technical regulations (TR) cover multiple aspects, from cryptographic requirements to the security of mobile applications used to access the data to how patient information must be maintained and accessed digitally.

IT Security Act 2.0

The IT Security Act 2.0 came into force in 2021 and expanded the requirements for securing access to data and systems that process Social Data as part of critical infrastructure.

Branch Specific Security Standard (B3S)

The B3S is an overarching security requirement for all hospitals over a specific size. In 2021, the BSI published the B3S, which contained requirements for all hospitals processing over 30,000 patients annually. The B3S includes 168 standards that applicable hospitals must implement and a review every two years for hospitals to demonstrate that they comply.

Bundesdatenschutzgesetz (BDSG)

With the advent of the General Data Protection Act (GDPR) in the EU and other German-specific privacy regulations such as the BDSG, German healthcare organizations must follow strict privacy stipulations.

Example German Healthcare Use Cases

There are many healthcare use cases specific to Germany. Here we'll explore a few, including data protection, system resiliency, and system security.

Data Protection

The Digital Healthcare Act (DVG) does not have explicit security requirements; however, it has been the catalyst for German healthcare organizations to begin providing patients with digital access to their data. Digitally stored data often includes:

- Administrative and demographic information
- Patient diagnosis
- Treatment information
- Prescription drugs
- Hospitalization info
- Patient insurance

Because of the SGB, these types of data, defined as "Social Data," fall under the regulations defined by Gematik, PDSG, and the TRs. Under this regulatory structure, organizations such as insurance companies and digital health application developers storing these data types are now within the scope of the Gematik, PDSG, and TRs requirements.

The SGB breaks Germany's Telematikinfrastruktur into three sections:

1. Centralized Infrastructure
2. Decentralized Infrastructure
3. Application Infrastructure

According to SGB V, healthcare providers are responsible for securing data transmission from their decentralized infrastructure to the centralized infrastructure. For example, they must secure their Telematik connectors against unauthorized access and utilize state-of-the-art encryption methods when transferring data. Additionally, organizations must store Social Data in German data centers and not transmit it outside the country.

These regulations are summarized into the following requirements around data security:

- **Encryption at Rest** - Social Data must be stored using state-of-the-art encryption methods
- **Encryption in Transit** - Social Data must be encrypted using state-of-the-art encryption methods as it is transmitted
- **Key Management** - Cryptographic keys must be stored securely and rotated regularly
- **Data Location** - Social Data cannot leave the country. Regulations require that all relevant sensitive data must be stored and hosted in data centers within Germany

- **Data Privacy** - Users must consent to the storage of their data, they must be able to access their data, and request a 30 day deletion of their data

How Google Cloud Can Help

Google Cloud provides a variety of built-in controls and tools which help to address the concerns and requirements raised by German regulations around the management of Social Data.

Encryption at Rest

Regulations such as the TRs and the PDSG require that all stored Social Data be encrypted with state-of-the-art encryption. Google Cloud natively encrypts all customer content stored at rest, without any action from the customer, using one or more encryption mechanisms. We use several layers of encryption to protect data. Data is encrypted at both the storage system layer and the storage device layers, and backups are encrypted. Using Cloud Key Management Service (KMS), you can create, rotate, track, and delete keys. With customer-managed encryption keys (CMEK), customers can use keys that they manage to protect data within Google Cloud.

Using CMEK gives customers control over more aspects of the lifecycle and management of your keys, including preventing Google from being able to decrypt data at rest, along with supporting integration with several additional encryption tools such as Cloud HSM (hardware-backed) keys and Cloud External Key Manager (EKM) keys. These integrations allow organizations to implement the right tool based on their data security strategy. Healthcare customers can find more information on Google Cloud's encryption practices here.

Encryption in Transit

The TRs and the PDSG require that Social Data be encrypted in transit, mainly as data travels between centralized, decentralized, and application infrastructure. Google Cloud employs several security measures to help ensure the authenticity, integrity, and privacy of data in transit. We encrypt and authenticate data in transit at one or more network layers when data moves outside physical boundaries we do not control. All VM-to-VM traffic within a VPC network and peer VPC networks is encrypted.

Customers with additional data encryption requirements over WAN can implement further data protection as it moves from a user to an application or virtual machine. These protections include IPSec tunnels, Gmail S/MIME, managed SSL certificates, and Istio. Customers can find more information regarding Google Cloud's practices around encryption in transit here.

Key Rotation

The TR's and PDSG require regular data encryption keys (DEK) rotations. We store the keys near the data they encrypt because of the volume of keys we store and the need for low latency and

high availability. The DEKs are encrypted with (or "wrapped" by) a key encryption key (KEK). One or more KEKs exist for each Google Cloud service. These KEKs are stored centrally in Google Cloud's KMS - a repository explicitly built for storing keys. The smaller number of KEKs than DEKs, coupled with using a central key management service, makes storing and encrypting data at scale to be manageable. This structure allows us to track and control data access from a central point while meeting all regulatory key rotation requirements. We share additional key management process information here.

Data Location

Gematik's requirements outline the data locality requirements in Germany. To support our customers' data residency requirements, Google Cloud enables customers to store their data for specific services in the region of their choice. German customers using data residency services can store customer data at rest exclusively within Germany and set up a Resource Locations organization policy that constrains the location of new resources for their whole organization or individual projects. With these capabilities, customers can prevent their employees from accidentally storing Social Data in an unintended Google Cloud region. Customers can find more information regarding data residency services here.

If you are using Cloud KMS, your cryptographic keys will be stored in the region where you deploy the resource. Customers can store those keys inside a physical Hardware Security Module located in the region you choose with Cloud HSM. Alternatively, if you use a local External Key Manager (EKM), you can place the key in a geographic location of your choice, under either your control or that of a domestic partner, and the key will be stored and managed in a third-party product deployed outside our infrastructure.

Additionally, Assured Workloads offers support for regulatory compliance by helping to manage the requirements for your regulated workloads with just a few clicks, reducing overall costs and risk through simplified management of required controls. Assured Workloads can help accelerate your path to running more secure and compliant workloads on Google Cloud by allowing you to control the regions where data at rest is stored. You can create an environment and select your compliance regime during Assured Workloads setup. When you create resources in the environment, Assured Workloads restrict the regions you can select for those resources based on the compliance regime you chose using the Organization Policy. Customers can find more information on Assured Workloads platform here.

Data Privacy

Data privacy is a priority for German regulators, specifically under BDSG, which outlines specific privacy requirements aligned to GDPR. Google Cloud is committed to data privacy and transparency, our Cloud Data Processing Addendum (CDPA) clearly articulates our privacy commitment to customers. Our transparent Privacy Principles:

- **You control your data** - Customer data is your data, not Google's. We only process your data according to your agreement(s).
- **We never use your data for ads targeting** - We do not process your customer data to create ads profiles or improve Google Ads products.
- **We are transparent about data collection and use** - We're committed to transparency, compliance with regulations like the GDPR, and privacy best practices.
- **We never sell customer data or service data** - We never sell customer data or service data to third parties.
- **Security and privacy are primary design criteria for all of our products** - Prioritizing the privacy of our customers means protecting the data you trust us with. We build the strongest security technologies into our products.

Any data that a customer puts into Google Cloud will only be processed in accordance with the customer's instructions, as described in our data processing agreements. Administrators can export customer data, via the functionality of the Google Workspace or Google Cloud services, at any time during the term of the agreement. We include data export commitments in our data processing terms and will continue to work to enhance our data export capabilities, making it even easier for you to download a copy of your customer data from Google Workspace and Google Cloud services. You can delete customer data, via the functionality of the Google Workspace or Google Cloud services, at any time.

Additionally, Google Cloud provides Access Transparency and Access Approval logging to help expand visibility and control over your cloud provider with admin access logs and approval controls. Google Cloud does not access customer data for any reason outside of contractual obligations, and we require a valid business justification for any access by support or engineering personnel. Near real-time logs offer insight into when Google Cloud administrators access your data. You can approve or dismiss requests for access by Google Cloud employees working to support your service. More information about our privacy commitments can be found here, and information about Google's Access Transparency can be found here.

Data Sovereignty

Combining location, encryption, privacy and transparency capabilities in one offering, Google Cloud offers Sovereign Controls either directly or through a domestic partner, like T-Systems in Germany. "Sovereign Controls by Google" and "Sovereign Controls by Partners" are two variations of this principle, which leverage external management of the encryption keys and additional optional services from the operating partner.

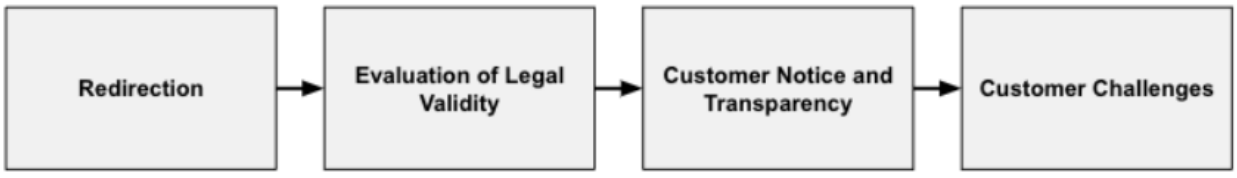
Sovereign Controls by Partners provides controls to address sovereignty requirements with partner operations and assurance

- **Data residency controls**
  Customer data will be stored at rest and workloads will be executed in partner's region and data will be restricted from moving outside of the region
- **Personnel controls**
  Personnel access and customer support is restricted to EU persons located in the EU. This is generally partner personnel.
- **External key management & access justifications**
  Keys encrypting customer data are stored and managed by the partner outside Google Cloud's infrastructure. Partner defines key access policies and monitors justifications.
- **Admin access control & transparency**
  Administrative access to customer data and workloads is logged, audited, and permitted only under predefined conditions. Partner defines access policies and monitors / audits access.
- **Additional - optional - partner controls**
  Optional additional controls and security services can be offered by each partner (BYOID, SOC, professional services ...)

In any case these are easily deployable over the customers` cloud architecture by simply grouping the relevant cloud resources (data, workloads and cloud services) into a dedicated folder, upon which the adequate compliance policies are applied.

Government Access

Foreign government access to sensitive data, such as Social Data is a concern for German regulators. Like many technology companies, Google Cloud receives requests from governments and courts to disclose customer information. Most requests are issued in the context of criminal investigations, but government agencies may also request information of civil or administrative cases. Google Cloud has strong operational policies, procedures, and other organizational measures to protect against unlawful or excessive requests for user data by public authorities. Our approach to government requests for information, regardless of the type of request, follows the same steps unless prohibited by or unreasonable under the applicable laws.



- **Redirection** - If we receive a request from a government agency for Cloud customer data, we inform the government that it should issue the request directly to the organization in question.

- **Evaluation of Legal Validity** - If the government compels Google Cloud to respond to a request for customer data, a dedicated team of Google Cloud lawyers and specially trained personnel will carefully review the request to verify that it is lawful, proportionate, and satisfies Google Cloud's policies.
- **Customer Notice and Transparency** - We will notify the customer before their customer data is disclosed unless such notification is prohibited by law, could obstruct a government investigation, or lead to death or serious physical harm to an individual.
- **Customer Challenges** - We will, to the extent allowed by law and by the terms of the government request, comply with a customer's reasonable requests regarding its efforts to oppose a request, such as the customer filing an objection to the disclosure with the relevant court and providing a copy of the objection to Google Cloud.

Our customers should have confidence that government requests of any nature will be subject to a transparent legal framework that requires government agencies to first seek data directly from customers and guarantees due process for customers and service providers. Google Cloud continues to monitor and support the developments with the Transatlantic Framework and will continue to advocate for reasonable limits on government surveillance. More information about our government access policies can be found here.

If the customer is using an external key management system (EKM) coupled with Key Access Justification (KAJ), or Sovereign Control by Google or by a domestic partner, an additional layer of protection is provided, as the customer may refuse access to the encryption key protecting their data for any reason (including a lack of reason would be prevented from providing a reason.

System Resiliency

Healthcare organizations store and maintain highly critical information that can be accessed at any time. Hospitals or other healthcare providers mainly rely on quick and reliable patient data access to provide their patients with the best possible treatment. Any delays or downtime in accessing their systems or patient data could risk patient lives. As a result, the Gematik and TRs define strict requirements for the uptime and accessibility of healthcare systems. Both regulations require that key systems must be offline for less than 1 minute per month (99.99% availability). Still, because any potential outages or downtime could cause major medical issues for their patients, this requirement is only the baseline, and providers typically aim for as high of a percentage as possible.

How Google Cloud Can Help

Google Cloud provides a variety of built-in controls and tools which help to address the concerns and requirements raised by German regulations around the resiliency of systems utilized by HCLS organizations.

Resiliency & Availability

From a regulatory perspective, Gematik and TRs require that key systems be offline for less than one minute per month. We know this level of availability is important to healthcare customers and design our data centers and network architecture for maximum reliability and uptime. Our computing platform assumes ongoing hardware failure and uses rigorous software failover to survive disruption.

Furthermore, our engineers proactively identify dependencies in our systems and redesign to eliminate them. Data is replicated multiple times across Google Cloud's clustered servers so that, in the case of a machine failure, data will still be accessible through another system. Customer workloads are securely distributed across multiple regions, availability zones, points of presence, and network cables to provide robust built-in redundancy and application availability.

Google Cloud runs one of the largest private networks in existence, minimizing risk for customers. This fully software-defined network allows us to scale reliably, providing our customers consistent service 24/7/365. Some infrastructure and solutions that support consistency of service:

- Three zone minimum per region for resiliency
- Multi-region replication and failover
- Zero planned downtime with Live Migration
- 24/7/365 world class monitoring and detection with full transparency
- Application service deployment trust mechanisms, built for multi-tenant service from inception
- Hardened physical premises with purpose-built servers and custom security chips

For more information on Google Cloud's availability, see the list of Service Level Agreements here.

Backups and Data Replication

Similar to availability, Gematik and the TRs both contain backup requirements for systems containing Social Data. To help our customers achieve compliance withGematik and the TRs, we offer a broad range of data protection features such as:

- Backup for GKE
- Persistent Disk snapshots
- Cloud SQL backups
- Filestore backups
- Geo-redundant Cloud Storage

Customers and independent software vendors (ISV)s can use these features to design and implement strong protection strategies. Additionally, a broad ecosystem of ISV and system integration (SI) partners provide backup and disaster recovery offerings on, and integrate with,

Google Cloud. This provides our customers freedom of choice and facilitates frictionless use of preferred third-party products and services. More information around Google Cloud's backup and disaster recovery solutions can be found here.

Network and Application Resilience

Google Cloud's Load Balancing allows for simplified deployment and easily scalable resources with high availability. Cloud Load Balancing provides cross-region load balancing, including automatic multi-region failover, and can react instantaneously to changes in users, traffic, network, backend health, and other related conditions. This allows healthcare organizations to scale as their users and traffic grow, and to handle any unexpected spikes by diverting traffic to other regions that can handle the traffic. More information about Google Cloud's load balancing solutions can be found here.

Incident Response

Gematik and TRs outline requirements for responding to data breaches or security incidents, such as reporting, collecting, and retaining relevant logs for analysis. Incident response is a crucial aspect of our security and privacy program, and we have a rigorous process for managing security incidents. This process specifies actions, escalations, mitigation, resolution, and notification of any potential incidents impacting customer data's confidentiality, integrity, or availability. Customers can find more information about Google Cloud's tools to assist with responding to incidents here.

Secure Infrastructure

As mentioned above, Gematik and TRs require that key systems be offline for less than one minute per month, highlighting that infrastructure security is vital in ensuring that systems are resilient. Infrastructure security is typically designed in progressive layers starting from the physical safety of data centers, continuing to the protection of the hardware and software that underlie the infrastructure, and finally, the technical constraints and processes in place to support operational security.

By migrating to Google Cloud, customers can benefit from reduced cybersecurity risk and more resilient systems.

For example, both our server boards and networking equipment are custom-designed. They don't include unnecessary components like video cards or peripheral interconnects that can introduce vulnerabilities. We vet component vendors we work with and choose components with care, while working with vendors to audit and validate the security properties provided by the components.

Google Cloud infrastructure is fundamentally designed to be multi-tenant, and does not assume any trust between services running on the infrastructure. This 'zero-trust' model contrasts

significantly with the approach traditionally used in data centers, where reliance is placed on the external network perimeter to protect internal resources. Learn more about Google Cloud's secure infrastructure here.

System Security

Critical infrastructure is frequently the target of cyber attacks, and the German healthcare industry is increasingly at risk as they move into the digital world. Whether healthcare providers are subjected to ransomware attacks, German HCLS organizations are being targeted more. Any disruption to the healthcare industry not only has economic impacts, but has the potential to impact patient outcomes. These outdated systems have a large number of potential attack surfaces that can be exploited, and leaves HCLS organizations at a high risk for security breaches. As a result, German authorities have pushed for regulations requiring increased security requirements for all organizations in the healthcare space.

For all other HCLS organizations, other regulations such as SGB, PDSG, and the IT Security Act outline other security requirements for all critical infrastructure, which includes healthcare providers, payers, systems, and services. While there are minor differences between these regulations, they are built off the backbone of the ISO 27001 and 22301 regulations, including (on top of the topics listed above) the following critical requirements:

- **Access Control Requirements** - Access to data and systems processing information must be limited to users that require access to perform their duties
- **Configuration Management** - Systems must be securely configured in a secure manner in alignment with baselines aligned to security requirements
- **Logging and Monitoring** - Systems should be consistently logged and monitored via security event logs or other security monitoring controls
- **Security Incident Management** - Plans and processes must be in place to respond to any potential incidents or data breaches
- **Sensitive Data Management** - Data must be encrypted, and stored securely within Germany
- **Infrastructure Security** - Infrastructure must be securely designed with relevant security controls built-in

How Google Cloud Can Help

Google Cloud accelerates an organization’s digital transformation through data democratization, app and infrastructure modernization, people connections, and trusted transactions. The result is an organization—and its workers—that can take advantage of all the benefits of cloud computing to drive innovation. These capabilities allow for greater security compliance, and can

allow German HCLS organizations to take advantage of secure-by-design infrastructure, built-in protection, and a global network that Google Cloud uses to protect your information, identities, applications, and devices. Our stack builds security through progressive layers that deliver defense in depth at scale in a modernized cloud solution.

Regulatory Compliance

Google Cloud is committed to compliance with industry standards and regulations, such as ISO 27001 and BSI C5:2020, which is the Cloud Computing Compliance Criteria Catalogue developed by BSI as a way to assess the information security of cloud services. Our products and services regularly undergo independent verification of their security, privacy, and compliance controls, achieving certifications, attestations, and audit reports to demonstrate compliance. We've created a central Compliance Resource Center that captures our global documentation along with additional resource documents and mappings for compliance support when formal certifications or attestations may not be required or applicable.

Access Controls

The B3S and IT Security Act 2.0 contain requirements around securing access to all data and systems which process Social Data. Access can only be granted to users that require it to conduct their duties, and all other access must be restricted. Google Cloud's Identity and Access Management (IAM) tools lets administrators authorize who can use specific resources - giving you full control and visibility to manage Google Cloud resources centrally. For enterprises with complex organizational structures, hundreds of workgroups, and many projects, IAM provides a unified view into security policy across your entire organization, with built-in auditing to ease compliance processes. More information around Google Cloud's access control capabilities can be found here.

Configuration Management

B3S contains requirements that systems are deployed off of secured baselines. These baselines must be maintained and updated to ensure that they contain baseline security controls. Google Cloud Deployment Manager is an infrastructure deployment service that automates the creation and management of Google Cloud resources. Write flexible template and configuration files and use them to create deployments that have a variety of Google Cloud services, such as Cloud Storage, Compute Engine, and Cloud SQL, configured to work together. This allows for security controls to be deployed by default, and compliance reports to be generated for each VM deployed. More information around Google Cloud's configuration management tools can be found here.

Logging and Monitoring

These regulations stipulate that logs around security event logs should be kept and monitored. Google Cloud Logging is a fully managed service that performs at scale and can ingest application and platform log data, and custom log data from GKE environments, VMs, and other

services inside of Google Cloud. Log Analytics can provide troubleshooting, security, and business insights, incorporating the power of BigQuery into Cloud Logging. Cloud Monitoring provides visibility into the performance, uptime, and overall health of cloud-powered applications. Collect metrics, events, and metadata from Google Cloud services, hosted uptime probes, application instrumentation, and a variety of common application components. Visualize this data on charts and dashboards and create alerts so you are notified when metrics are outside of expected ranges. More information around Google Cloud's logging and monitoring solutions can be found here.

Security Incident Management

B3S outlines requirements for incident response plans and processes in order to respond to any potential incidents or data breaches. Incident response is a key aspect of Google Cloud's overall security and privacy program. See the Incident Response section above for more details around how Google Cloud can help healthcare organizations better respond to security incidents.

Sensitive Data Management

B3S contains requirements for data management, similar to the TRs and PDSG. These requirements range from encryption of data at rest and in transit to data location and privacy. The Data Security section above captures more information on our tools and capabilities for managing sensitive data. Additionally, customers concerned about the management of their sensitive data can also reference Google Cloud's Cloud Data Loss Prevention.

Cloud Data Loss Prevention provides you the means to manage your data on or off cloud, and it includes powerful tools that allow you to classify, mask, tokenize, and transform sensitive elements. With support for structured and unstructured data, Cloud DLP can tokenize or mask to help you preserve the utility of your data for joining, analytics, and AI while protecting the raw sensitive identifiers. Cloud DLP is integrated with many products such as Logging and BigQuery or can be used in your ETL and ELT pipelines.

Infrastructure and Network Security

B3S, PDSG, and the IT Security Act all contain requirements for securing the critical infrastructure used within the healthcare industry. Google Cloud has a global-scale technical infrastructure that's designed to provide security through the entire information processing life cycle. This infrastructure provides 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. See the Secure Infrastructure section above for more information around infrastructure security.

Additionally, we offer a comprehensive set of network security controls that allow you to adopt a defense-in-depth security strategy to minimize risk and ensure safe and efficient operations

while satisfying compliance requirements. By utilizing a zero trust security model where no one is trusted by default, access controls are shifted from the network perimeter to the users and devices. Various Google Cloud tools such as Cloud Armor enable you to allow, deny, or redirect requests to your external HTTP(S) load balancer at the edge, as close as possible to the source of incoming traffic. Cloud Armor also provides the means to filter out traffic from geographic locations and/or IP lists of known attackers. These policies prevent unwelcome traffic from consuming resources or entering your network, and segment and secure your cloud perimeter. More information around our network security capabilities can be found here.

Conclusion

As the German healthcare industry continues its path towards digital transformation, the need continues to grow for an underlying infrastructure which can securely and reliably handle the sensitive data being stored. Germany's numerous regulations continue to increase the controls and requirements healthcare organizations must adhere to in order to operate within the digital space. Consequently, these organizations are looking to partner with organizations whose products are scalable and secure, reliable, fault-tolerant, capable of low-latency delivery, all while meeting their patient, stakeholder, and regulator requirements.

Google Cloud has a track record of delivering on every front mentioned above, which is why many healthcare providers look to partner with us as they introduce their latest security and technological advancements to the market. Whether it be meeting privacy needs, operational resilience, or encryption of data, Google Cloud is committed to keeping in step with the continuously evolving needs of our customers in the German healthcare industry.