Google Cloud Whitepaper
May 2026

Building Software as a Medical Device (SaMD) on Cloud Infrastructure

Tamara Redondo, RK Neelakandan

Google Cloud

Table of contents

Introduction

Modern medical devices are increasingly composite systems, where clinical functionality emerges from the interaction of embedded firmware, mobile applications, and cloud-based services. For manufacturers in regulated environments, this architectural complexity raises a fundamental question: How can these composite systems provide the level of control and 'State of Control' required for medical device certification? When a system's components are distributed across different environments, each with its own failure modes, quality, regulatory, and security teams must demonstrate that system integrity, auditability, and operational oversight remain intact throughout the product lifecycle.

This paper is intended for quality, regulatory, and security teams evaluating cloud infrastructure medical device programs. It examines how cloud services can support the operational controls required for regulated environments, including identity governance, infrastructure traceability, system monitoring and controlled deployment environments. As the first in a series covering the full lifecycle of medical device systems with a presence in the cloud, this work establishes the foundational infrastructure through development and operational security.

In these distributed systems, where clinical functionality is spread across firmware, mobile apps, and cloud services, understanding the boundary between infrastructure platform and the regulated device is essential. While the cloud provider manages the security *of* the cloud (the physical facilities and foundational services), the manufacturer's specific configuration and software transform that "utility" into a "medical device." Consequently, the platform boundary remains a matter of shared fate: the cloud provides the primitives for control, but the accountability for device safety, quality systems, and regulatory submissions remains entirely the manufacturer's responsibility.

We demonstrate that cloud infrastructure is not merely an acceptable alternative to on-premises servers; it is a superior foundation for Software as a Medical Device (SaMD) and digital health systems. When treated as a control platform, cloud makes governance enforceable and evidence continuously available. The paper's organizing construct is a three-plane framing:

- The data plane covers how clinical or device data moves through the system to deliver intended functionality
- The control plane defines how the system is governed: identity, network boundaries, release gates, and configuration constraints that prevent unauthorized or unintended change.
- The evidence plane captures the objective record of what the system does and how it is governed: immutable audit trails, build and deployment attestations and ongoing monitoring history.

This framing clarifies the distinction between regulatory accountability and technical enforcement. While the manufacturer retains full regulatory accountability for device safety and quality systems, the cloud platform provides the technical primitives, such as centralized identity, network segmentation, and immutable auditing, used to implement those requirements. By configuring these primitives into a "State of Control," the manufacturer transforms administrative policies into system-enforced behaviors, producing defensible evidence artifacts as an automated byproduct of operations.

Disclaimer

This document reflects industry practices, regulatory interpretations and technology capabilities as of May 2026. Given the evolving nature of regulatory guidance, cloud technologies, and AI/ML frameworks, readers should consider this content as a point-in-time perspective. Organizations are responsible for ensuring alignment with current regulations and internal policies.

Regulatory Context

Across jurisdictions, the most cloud-relevant regulatory requirements are rarely phrased as “must be on-premise” or “must be on-cloud.” Instead, they focus on whether the manufacturer can demonstrate effective control of the system, including cybersecurity, traceability, verification and validation discipline and postmarket responsiveness.

EU Medical Device Regulation

Under EU MDR, Annex 1, Section 17.2, it is explicit that manufacturers must treat software engineering and security as lifecycle obligations. Software must be developed in accordance with the state of the art considering development lifecycle principles, risk management, and verification and validation. Manufacturers must also define minimum requirements for hardware, IT network characteristics, and IT security measures necessary for the software to run as intended.

MDCG 2019-16 Rev.1 cybersecurity guidance applies these European Union Medical Device Regulation (MD) concepts across the device lifecycle, including expectations for verifying security controls and practical considerations such as log storage and backup. It also emphasizes that security requirements for the operating environment must be clearly documented and risk-based.

United States: FDA QMSR and Cybersecurity Guidance

The FDA’s Quality Management System Regulation (QMSR) final rule (effective February 2, 2026) harmonizes 21 CFR Part 820 with ISO 13485:2016. This alignment reinforces the practical value of adopting cloud-native infrastructure patterns that automate document control, change management,

and supplier oversight. By transitioning from manual paperwork to repeatable, system-enforced behaviors, manufacturers can generate objective evidence as a continuous byproduct of their operations.

FDA's Cybersecurity in Medical Devices guidance (issued September 2023) is directly relevant to cloud-based architectures. It encourages manufacturers to use a Secure Product Development Framework (SPDF) as a way to reduce vulnerabilities throughout the total product lifecycle and explicitly connects cybersecurity practices to QMS expectations. It also describes SBOM expectations and, for "cyber devices", notes that SBOMs are required under FD&C Act section 524(b)(3). A Secure Product Development Framework (SPDF) is a set of processes that help identify and reduce the number and severity of vulnerabilities in products. It encompasses all aspects of a product's lifecycle, including design, development, release, support and decommission.

To meet the rigorous Software Bill of Materials (SBOM) and vulnerability management requirements of FD&C Act Section 524B, manufacturers can leverage the Supply Chain Levels for Software Artifacts (SLSA) framework, a security standard pioneered by Google. By utilizing Google Cloud's Software Delivery Shield, Artifact Registry, and Cloud Build, organizations can automatically generate SLSA-compliant provenance. This mathematically proves to regulators that the SaMD source code was not tampered with during the build process, automating a massive portion of the FDA's cybersecurity premarket expectations.

FDA's premarket software documentation makes regulatory evidence patterns concrete. It recommends lifecycle artifacts that map naturally to cloud-native pipelines and infrastructure governance, including software requirements specifications, risk management files, architecture diagrams, configuration management practices, V&V testing documentation, and software version history.

FDA's Computer Software Assurance (CSA) guidance is highly relevant to cloud foundations used for production and QMS software. It describes a risk-based approach to establishing confidence in software used in production or QMS contexts, and explicitly notes that digital retention, automated traceability, systems, and audit trails can be used as objective evidence, reducing reliance on manual or paper processes.

International Convergence

IMDRF's SaMD QMS guidance reinforces that QMS practices include governance processes such as document and record control, configuration management, and management of outsourced processes, and makes the accountability model explicit, even when components or code are supplied by others, the manufacturer remains ultimately responsible for safety and performance.

For digital health systems that handle protected health information, HIPAA is often an adjacent governance requirement. HHS office for Civil Rights guidance reinforces the broader compliance reality:

cloud does not remove obligations, it changes how they are implemented and contracted. Entering into a Business Associate Agreement is not sufficient, as the covered entity remains responsible for implementing compliance controls.

The Three-Plane Model

This paper is intentionally framed across three planes: a data plane, a control plane and an evidence plane. This separately clarifies a core point for regulated environments: effective control is not only implemented once, it is continuously evidenced through system-generated records.

Plane	What it covers	Why it matters for regulated systems
Data Plane	How clinical or device data moves through the system to deliver intended functionality	Defines the functional boundary of the device system and what must be secured and validated
Control Plane	Identity, network boundaries, release gates, and configuration constraints that prevent unauthorized or unintended change	Provide the enforcement mechanisms that quality and security teams rely on to demonstrate operational control
Evidence Plane	Immutable audit trails, build and deployment attestations and ongoing monitoring history	Produces the objective records that support audit, inspection and submission review, continuously and as a byproduct of normal operations
Example: PHI ingestion API	HTTPs endpoint receiving physiological sensor data from the mobile app, routes to processing service and encrypted storage	Control plane: IAM restricts which service accounts may call the endpoint: VPC firewall limits ingress to authorized sources

Cloud Capabilities Mapped Controls

Cloud governance follows a shared fate model: the provider secures the cloud (facilities, hardware, foundational services), while the manufacturer configures and secures what they run in the cloud (identities, policies, workloads, data handling, SDLC, validation evidence). For medical devices, that translates to a practical rule-the platform can provide strong primitives and auditable telemetry, but the manufacturer must implement and validate their intended controls and evidence strategy.

As an example of this shared fate model, Google Cloud's HIPAA compliance material states that entering into a BAA is not sufficient by itself, the covered entity is responsible for building a compliant solution and implementing compliance controls. This is aligned with IMDRF's view that manufacturers remain responsible for safety and performance even when relying on external components.

Foundational Control Mapping

The table below maps control objectives, the questions auditors and regulators actually ask, to specific Google Cloud capabilities and the evidence artifacts produced.

Control Objective	Google Cloud Capability	Objective Evidence (Artifacts)	Regulatory Alignment
Least-privilege access & separation of duties	**Cloud IAM** (Custom Roles & Conditions)	IAM Policy Exports, Access Transparency Logs	**US:** 21 CFR Part 11.10(d) **EU:** Annex 11, Sec. 12 **Intl:** ISO 13485:2016 (7.3.7)
Network isolation & controlled ingress/egress	**VPC Service Controls** (Service Perimeters)	VPC-SC Policy Logs, Network Firewall Rules	**US:** FDA 2025 Cyber Guidance (Secure Arch) **EU:** MDR Annex I (17.2) **Intl:** IEC 62304 (Security)
Encryption key control & cryptographic governance	**Cloud KMS** (CMEK / Cloud HSM)	Key Rotation Logs, Cloud HSM Attestations	**US:** 21 CFR 11.10(h) **EU:** GDPR Art. 32 / MDR GSPR 17.1 **Intl:** ISO 27001 (A.18.1.5)
Immutable audit trails for admin change control	**Cloud Audit Logs** (Admin Activity)	Non-deletable Log Sinks, Log Integrity Exports	**US:** 21 CFR 11.10(e) **EU:** Annex 11, Sec. 9

			Intl: IMDRF N81 (Traceability)
Traceable software supply chain	**Binary Authorization** & Artifact Registry	Attestation Reports, Signed Container Images	**US:** FDA 524B (SBOM Requirements) **EU:** MDR Art. 10 (QMS Traceability) **Intl:** IEC 62304 (SOUP Mgmt)
Continuous monitoring & operational oversight	**Security Command Center** (SCC)	SCC Compliance Reports, Real-time Findings	**US:** FDA Post-market Surveillance **EU:** MDR Annex XIV (PMS) **Intl:** ISO 14971 (Risk Monitoring)
Guardrails to prevent non-compliant configurations	**Organization Policy Service**	Org Policy Snapshot, Constraint Enforcement Logs	**US:** FDA CSA (State of Control) **EU:** Annex 11, Sec. 10 (Change Mgmt) **Intl:** ISO 13485 (Maintenance)

Modern SaMD systems are not architecturally self-contained; they involve patient mobile apps, remote clinician dashboards, and third-party APIs. To secure these interactions, Google Cloud natively applies a Zero Trust architecture. Instead of relying on traditional network-based isolation (like a VPN or vLAN), which assumes anything "inside" the perimeter is safe, the control plane utilizes Identity-Aware Proxy (IAP) and Context-Aware Access. Access is granted only after evaluating a "composite" set of signals: the user's identity, the specific security posture of their physical device, and their geographic location. This shift from network-perimeter security to identity-and-context-based authorization directly supports HIPAA and GDPR mandates by ensuring that clinical data access is both granular and cryptographically verified, regardless of the user's physical network.

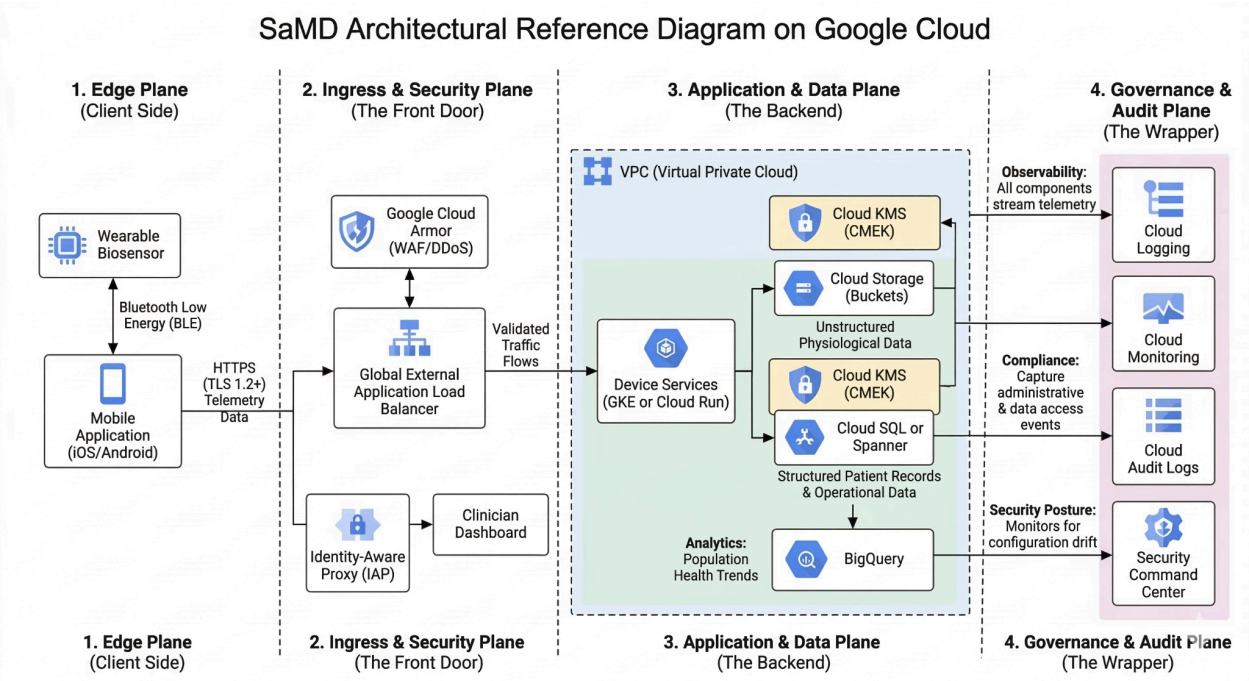
Representative Architecture

There is a broader shift underway in how regulated organizations approach Compliance, and this architecture is an expression of it. Historically, regulatory compliance in medical device development has been treated as a documentation discipline: a set of procedures, records, and reviews that run alongside engineering and are assembled into submissions. Controls were described in SOPs. Evidence was gathered after the fact. Audit readiness was a periodic exercise. This model worked when systems were simpler and change was slower, but it scales poorly into connected, continuously updated device platforms where the pace of change outstrips the capacity for manual administrative control.

What is emerging in its place is a convergence of DevSecOps principles and regulatory compliance practice. In this model, compliance is not described in a document that sits beside the system, it is expressed programmatically and enforced declaratively within the system itself. Controls are implemented as platform policy, not procedure. Change control is enforced at the pipeline gate, not reviewed after the fact. Evidence is generated operationally, as a continuous byproduct of how the system runs, rather than assembled administratively before an inspection. The quality system does not audit the engineering process from the outside, it is woven into it.

This is not simply a technology argument. It is a governance argument that the most defensible evidence of control is a system that cannot operate outside its controls, rather than a system that is periodically checked for compliance. FDA's CSA guidance gestures toward this in its endorsement of automated traceability and operational audit trails as objective evidence. The architecture below makes it concrete.

The representative architecture below is intentionally audit-shaped. Every major data path has a corresponding control and evidence path. This is the operational meaning of "compliance-as-code"—where objective audit evidence is generated automatically as a byproduct of normal operations, rather than through manual administrative burden.



The architecture spans the three planes described earlier. At the edge, a wearable sensor transmits physiological data over a local link to a mobile application. The mobile application communicates with the Google Cloud environment over HTTPS (TLS 1.2+) through a Global External Application Load Balancer, which serves as the controlled ingress point.

Within the cloud environment, device services receive and process telemetry, storing raw data in Cloud Storage and operational data in Cloud SQL or Spanner, both encrypted at rest using customer-managed encryption keys via Cloud KMS. Processed data flows to Big Query for analytics and to a clinician dashboard protected by Identity-Aware Proxy (IAP). Every ingress and service interaction generates entries in Cloud Audit Logs and Cloud Logging, which feed Cloud Monitoring for alerting and operational oversight.

The architectural separation of the data and control planes ensures that clinical data flows remain independent of governance updates, such as identity policies or deployment gates. This decoupling enables the evidence plane to operate continuously, where audit logs, monitoring alerts, and build attestations are generated automatically as a byproduct of normal operations. By shifting from periodic manual checks to system-enforced evidence generation, manufacturers can maintain a persistent "State of Control" without adding administrative burden to clinical workflows.

Quality, regulatory, and security teams typically need to defend the following questions during audits or submission reviews. The architecture creates an evidence trail for each:

Audit / Regulatory Question	Regulatory/SOP Requirement (The "Test")	Architectural Mechanism (The Enforcement)	Technical Evidence Artifact (The Proof)
Who can change the system?	*SOP-01: Principle of Least Privilege & Identity Verification*	**Centralized IAM & IAP:** Access is restricted by identity and device context.	**Immutable Admin Activity Logs** and IAM Policy Troubleshooter exports.
How are changes controlled?	*SOP-02: Software Integrity & Change Control (SDLC)*	**CI/CD Pipelines with Binary Authorization:** No code is deployed without a signed attestation.	**SLSA Provenance Metadata** and signed Attestations in Artifact Registry.
How is data protected?	*SOP-03: Data Encryption & Key Governance*	**CMEK via Cloud KMS:** Data is encrypted with keys managed by the manufacturer, not the provider.	**Key Access Justification (KAJ) logs** showing every decryption event and reason.
How is the environment constrained?	*SOP-04: Infrastructure Configuration Standards*	**Organization Policy Service:** Prevents the creation of non-compliant	**Denial Audit Logs** and Policy Snapshots proving the "State of Control."

		resources (e.g., public buckets).	
How are operations monitored?	*SOP-05: Continuous Post-Market Oversight*	**Cloud Monitoring & Error Reporting:** Real-time detection of clinical or security anomalies.	**SLI/SLO Dashboards** and Automated Incident Logs for post-market files.

Risk and Mitigations

The risks in this section are not unique to the cloud. Misconfiguration, evidence gaps, and unclear accountability have accompanied every generation of enterprise technology, from on-premise data centres to early virtualization platforms. What has changed is the obligation and the opportunity that comes with it.

Google's shared fate model is a direct response to this history. Shared fate means that Google has an engineering stake in customer outcomes, not just contractually. The design goal is that the safe configuration is the default configuration: guardrails are built in, insecure options require deliberate override and the platform surfaces risk before it becomes a problem. This is a fundamentally different posture from simply documenting what customers must do and leaving the outcome to them.

The risks below are presented not as customer failures but as areas where the platform, in partnership with the manufacturer, is engineered to reduce the likelihood of error. Where a risk remains, it is because the manufacturer must make a deliberate choice, about architecture, process or governance. The distinction matters, Google can engineer away accidental misconfiguration, but only the manufacturer can define what correct configuration means for their specific device, intended use and quality system.

Misconfiguration and Policy Drift

Teams creating resources outside approved baselines, such as the wrong regions, public exposure or weak IAM, directly undermine the MDR-style "minimum IT security measures" and create significant audit friction.

- Mitigation: Enforce **Organization Policy** **constraints** at the organization or folder scope to programmatically prevent disallowed configurations. Standardize VPC segmentation and firewall rule baselines.
- Audit Evidence: **Policy-denied audit logs** and Organization Policy snapshots serve as objective evidence that guardrails are active and enforcing the "State of Control."

Insufficient Audit Trail Coverage and Over-Privileged Access

Audit evidence often exists for administrative changes, but granular data access events (e.g., who viewed a specific patient record) may go uncaptured. Furthermore, without strict IAM Least Privilege controls, administrative roles may inadvertently inherit access to clinical data, violating "need-to-know" privacy mandates like HIPAA and GDPR.

- Mitigation: Implement a dual-layer identity and logging strategy. First, enforce Least Privilege by using Custom IAM Roles that strictly separate administrative duties (managing the cloud) from clinical data access (viewing patient records). Second, enable Data Access Audit Logs for all storage and database services to create a non-repudiable trail of every interaction with sensitive data. Finally, establish controlled exports to a locked Cloud Storage bucket (WORM) to meet the 10+ year retention requirements common in EU MDR.
- Audit Evidence: IAM Policy Analyzer reports proving zero-overprivilege for admin roles, Data Access Logs linked to unique user identities, and verified Bucket Lock settings that prevent the deletion of audit evidence.

Supply Chain and Release Integrity Gaps

Unscanned or unverified artifacts reaching production create an inability to prove what was deployed and why. This violates the FD&C Act Section 524B statutory requirements for SBOM generation and vulnerability management.

- Mitigation: Use **Artifact Registry** **scanning** and **Binary Authorization**. Require cryptographically signed attestations before a container can be deployed.
- Audit Evidence:**Scan outputs**, **Provenance metadata** (linking the build to a specific source commit), and **Binary Authorization enforcement logs**.

Unclear Supplier or Platform Accountability

Assuming a cloud provider's certification (ie SOC 2) equals device regulatory compliance is a common point of failure. Following IMDRF SaMD QMS principles, outsourced elements do not remove manufacturer responsibility.

- Mitigation: Maintain an explicit **Shared Responsibility Statement** within your QMS. Document your supplier control and monitoring processes for Google Cloud as a critical supplier.

- Audit Evidence: A documented **Responsibility Matrix** and a **Supplier Evaluation Report** that bridges Google's infrastructure certificates with your device-specific controls.

Operational Auditability & MDCG Guidance

To meet the "state-of-the-art" expectations for cybersecurity and auditability, this architecture operationalizes MDCG 2019-16 Rev.1 (Guidance on Cybersecurity for Medical Devices). This guidance bridges the gap between the high-level GSPRs and technical execution.

MDCG 2019-16 Focus Area	Architectural Implementation	Evidence Artifact
Security by Design	Separation of Data, Control, and Evidence planes to minimize attack surface.	Architecture Diagrams & Threat Models.
Verification & Validation	**Binary Authorization** gates ensuring only "known-good" builds reach production.	Deployment Attestation Reports.
Detect & Respond	**Cloud Logging & Monitoring** capturing all administrative and data-access events.	Immutable Audit Trails & SCC Findings.
Information for Users	Documenting the "Minimum IT Requirements" for the cloud operating environment.	Instructions for Use (IFU) / Technical File.

Risk and Mitigations

Misalignment of Data Residency vs. Operational Risk While physical data residency is often a localized requirement, it is distinct from the legal requirements for Cross-Border Data Transfer (CDBT). Under the EU MDR, the manufacturer must also ensure that the chosen location does not introduce risks to system availability or clinical integrity.

- Mitigation: Utilize Google Cloud Assured Workloads to programmatically enforce Resource Location Restrictions (Residency). This ensures that clinical data at rest remains within the specified EU regions. For organizations with specific operational requirements, Assured Workloads can also restrict technical support access to EU-based personnel. These technical guardrails serve as supplementary measures that provide objective evidence for a Transfer Impact Assessment (TIA), helping to document the "State of Control" required by both the MDR and the manufacturer's GDPR data protection strategy.
- Audit Evidence: Assured Workloads compliance monitoring reports and Resource Location Policy snapshots. These artifacts prove that the technical boundaries of the "operating environment" (GSPR 17.2) are enforced and monitored.

Audit Evidence

The checklist below is written as a practical evidence pack aligned to what quality, regulatory and security leaders typically need for internal audits, inspections, or notified body reviews. It is not a substitute for a manufacturer's QMS procedures. It is an example of how cloud-produced evidence can support those procedures. The artifacts below are generated automatically by the platform as a byproduct of normal operations. The manufacturer's quality system determines which are required, how they are retained and how they are used as objective evidence in submissions and audits.

Governance & Control Domain	Objective Evidence Artifact	Google Cloud Source
Governance & Scope	Documented Shared Responsibility Matrix & BAA	Google Cloud Terms

Identity & Access (IAM)	Non-repudiable logs of who accessed administrative consoles.	**Cloud Audit Logs** (Admin Activity)
Network Controls	Proof of network isolation and perimeter enforcement.	**VPC Service Controls** & Firewall Logs
Encryption & Key Mgmt	Records of cryptographic key rotation and access.	**Cloud KMS** (Key Access Justification)
Logging & Audit Trails	Confirmation of immutable log retention and integrity.	**Cloud Storage** (Locked/WORM Buckets)
Software Supply Chain	Evidence that only scanned, validated code was deployed.	**Artifact Registry** & **Binary Authorization**
Monitoring & Post-Market	History of system uptime and security incident alerts.	**Cloud Monitoring** & **SCC Reports**

Conclusion

A cloud foundation is a superior basis for software-enabled medical devices when it makes security controls enforceable, environments repeatable, and audit evidence continuously available. This aligns with EU MDR expectations for state-of-the-art lifecycle security and minimum IT security measures, and with FDA's direction toward risk-based assurance and use of digital records as objective evidence.

The regulatory boundary remains unchanged: the manufacturer retains responsibility for device safety, quality systems and regulatory submissions. Cloud infrastructure provides the primitives that can be configured to implement and evidence those responsibilities, and capable of producing evidence automatically as a byproduct of normal operations, rather than as a separate, manual compliance activity.

Recommended Next Steps

The most important shift this paper argues for is not a configuration change, it is a strategic one. Cloud infrastructure, used well, fundamentally changes the level of effort required to meet regulatory expectations for SaMD and connected device platforms. Compliance controls that previously required dedicated teams, manual processes, and periodic reconstruction can be expressed architecturally, enforced automatically, and evidenced continuously. The starting point is not a task list; it is an architectural commitment to building the system this way from the ground up.

Once that commitment is made, the Three-Plane Model provides the strategic frame. Each plane points to a distinct priority:

- **Data Plane: Define the system boundary precisely and early.** Cloud enables SaMD platforms to integrate device telemetry, mobile applications, analytics, and clinician-facing services as a coherent, governed architecture rather than a collection of loosely connected components. The regulatory value of cloud here is not hosting—it is the ability to enforce consistent data governance, encryption, and access controls across every component of the system boundary from day one.
- **Control Plane: Express your controls as policy, not procedure.** The single highest-leverage action a manufacturer can take is to translate their access control, change management, and network security requirements directly into platform policy—IAM role bindings, Organization Policy constraints, Binary Authorization attestations, and VPC segmentation. When a control is enforced by the platform rather than described in an SOP, it cannot be bypassed accidentally, it does not drift between environments, and it does not require periodic re-verification. This is the cloud advantage that no on-premise architecture can replicate at scale.
- **Evidence Plane: Design for continuous audit readiness from the start, not as a retrofit.** Cloud Audit Logs, build provenance, monitoring history, and policy-denied events are generated automatically as the system operates. The manufacturer's strategic decision is to route, retain, and govern that evidence stream as a first-class output of the architecture—not an afterthought assembled before an inspection. Organizations that make this decision early find that regulatory submissions and audit responses become progressively less burdensome over time, because the evidence already exists and is already attributable.

By executing these steps, organizations move beyond theoretical compliance to a state of operational readiness. This positions the upcoming topics in this series, Secure Development and Operational Security, to build upon a technically robust and regulator-defensible infrastructure substrate.

What's Next

The SaMD Cloud Trilogy: A Roadmap

This paper has established the Foundational Infrastructure (Technical Robustness) required for a regulator-defensible cloud environment. To complete the digital health lifecycle, the upcoming papers will dive deeper into execution and advanced operations:

- Paper 2: Secure Development & Lifecycle Management (The Process)
    - *Focus:* Moving from infrastructure to the SDLC. We will explore how to integrate GxP-compliant CI/CD pipelines, automated V&V, and SBOM management into the developer workflow to ensure "Software Integrity by Design."
- Paper 3: Intelligent Operations & Scalable Governance (The Value)
    - Focus: We will discuss Agent-based monitoring and leveraging the Office of the Chief Security Officer (OCSO) to reduce operational toil and friction.