Playbook

How to achieve medical-grade connectivity with AWS

zühlke
empowering ideas

Why now?

Connected medical devices are reshaping how care is delivered, how outcomes are measured, and how MedTech companies compete.

The market is projected to double to over USD 150 billion by 2030 (Mordor Intelligence, 2025). Remote monitoring, AI-driven diagnostics, and real-time decision support are rapidly becoming baseline expectations, not differentiators.

Connectivity is no longer a feature. It's the foundation of MedTech value, and the enabler for becoming truly AI and data-driven.

Medical-grade connectivity spans nine tightly linked challenges, from regulatory compliance and cybersecurity to interoperability and operational excellence. A weakness in one area doesn't remain isolated. It delays approvals, increases risk exposure, or blocks clinical adoption.

The solution

This playbook presents Zühlke's proven approach to medical-grade connectivity on AWS:

- **An eight-stage architectural flow** that addresses all nine challenges systematically, from device authentication through to exception handling and recovery (Chapter 2).
- **Three organisational shifts** that are just as critical as the technology: breaking silos, automating compliance, and building cloud expertise through a modern Cloud Centre of Excellence (Chapter 3).
- **A three-phase roadmap** to take you from discovery to scale in 90 days, starting with a single use case and building toward a multi-device connected care platform (Chapter 4).

Executive readiness dashboard

The dashboard below contrasts a legacy connectivity approach with a truly medical-grade model across five strategic pillars. Your connectivity platform should be able to withstand scrutiny from regulators, hospital CIOs, and investors.

Pillar	Legacy	Medical- grade
Regulatory	Periodic manual audits; compliance as afterthought	Continuous automated validation; compliance by design
Security	Bolt-on security; shared credentials; reactive patching	Zero-trust architecture; device-level encryption; continuous monitoring
Interoperability	Proprietary protocols; siloed data; manual EHR entry	FHIR-native; standards-based APIs; automated EHR sync
Scalability	Single-site deployments; manual provisioning	Auto-scaling; edge processing; multi-region resilience
Operations	Reactive support; manual updates; no fleet visibility	Predictive monitoring; automated OTA; full fleet managemen

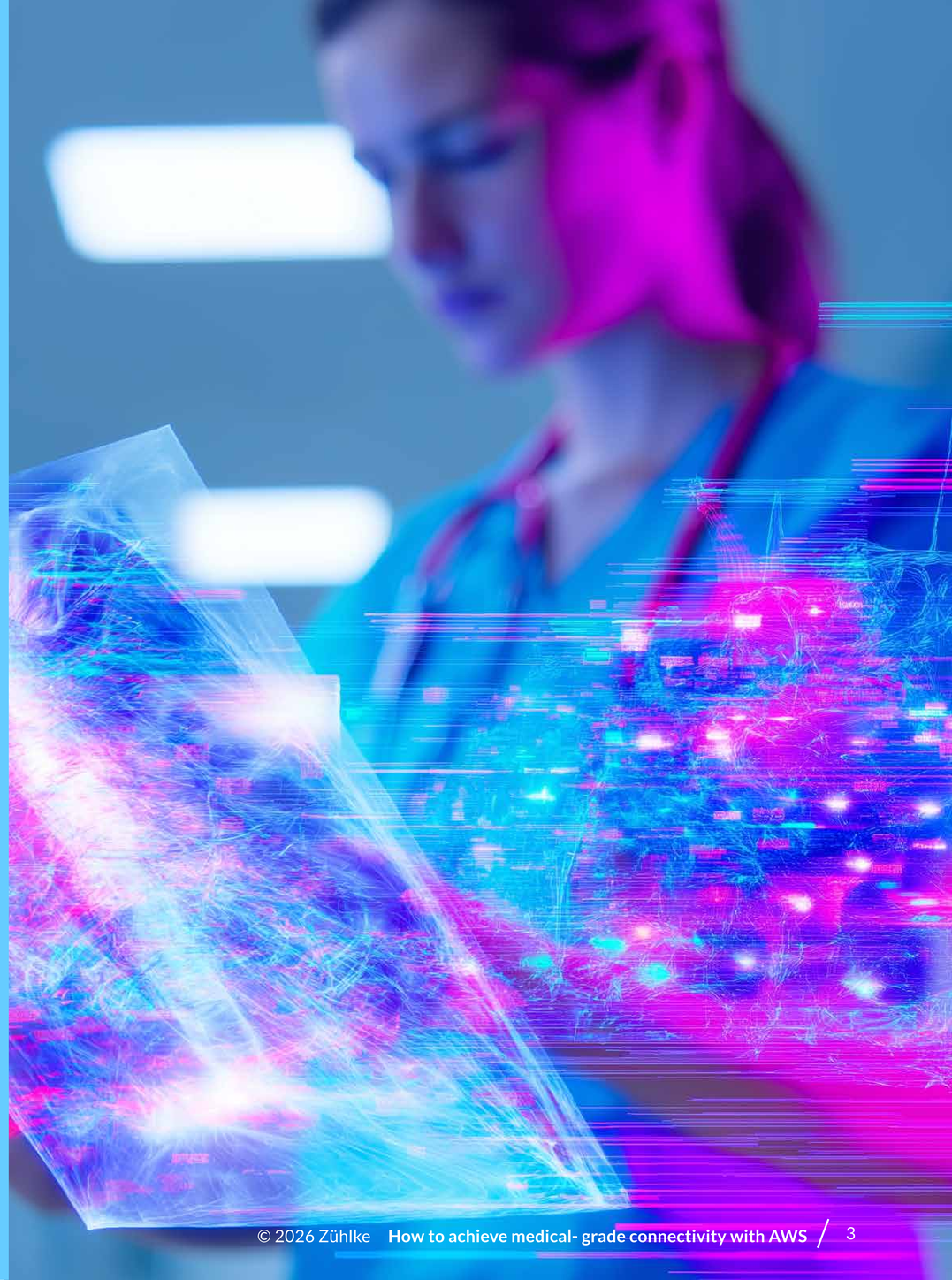
Your next 90 days: three action items

1. **Pick one use case and align your stakeholders (weeks 1 – 4)**. Choose a device where connectivity unlocks clear clinical or operational value. Get R&D, quality assurance, IT, and regulatory departments in the same room. Agree on success criteria and assess the regulatory impact.

2. **Build an end-to-end MVP on AWS (weeks 5 – 10)**. Implement the full eight-stage flow for your selected use case - including compliance and audit logging from day one. Validate the process with real clinical users.

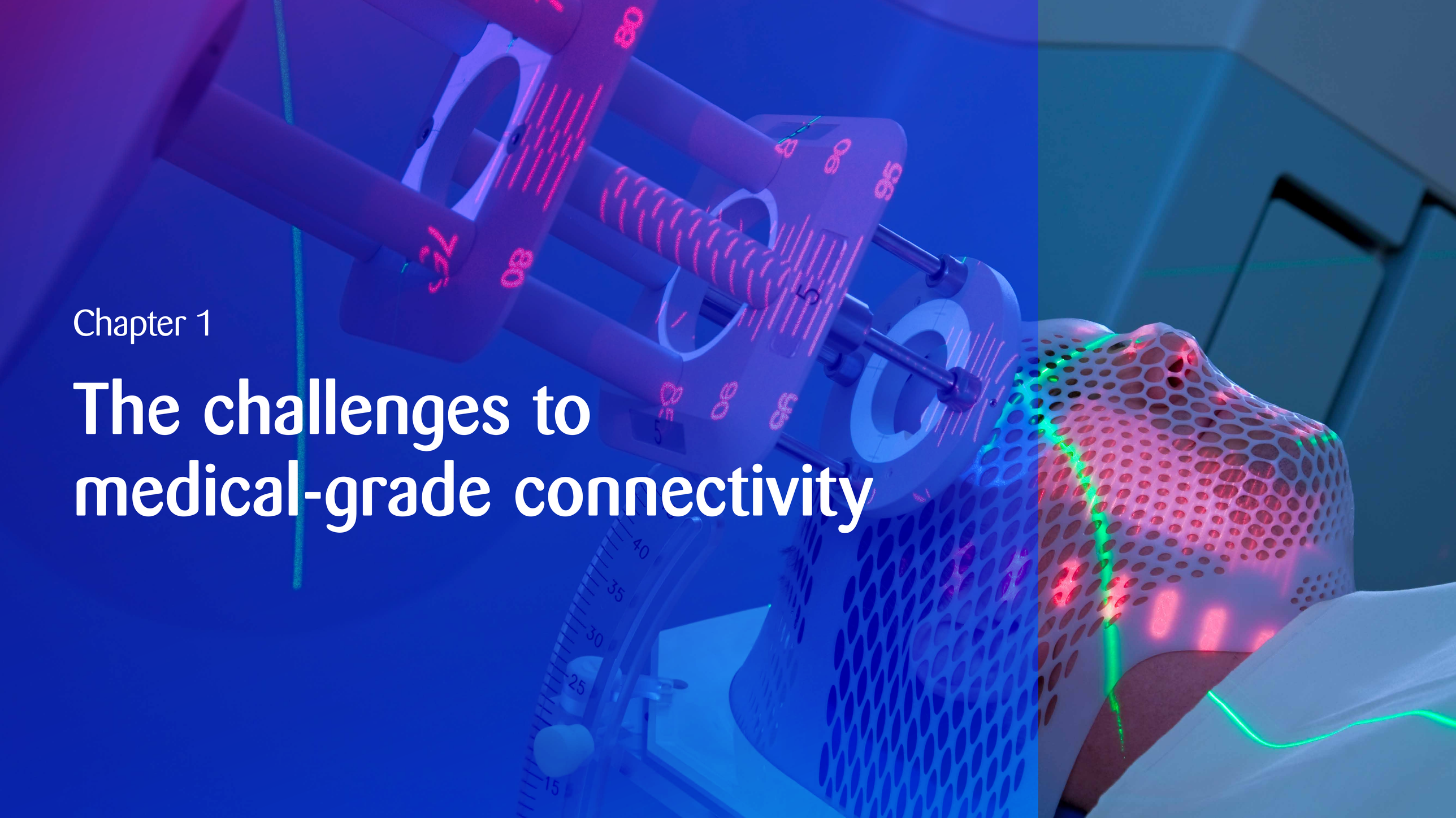
3. **Automate and scale (weeks 11+).** Move to policy-as-code and continuous validation. Expand to additional devices and markets. Invest in your Cloud Centre of Excellence to build lasting internal capability.

The complexity of medical-grade connectivity is real, but it's also what separates leaders from organisations still catching up. This playbook shows how to build scalable, secure, and compliant connected device platforms that unlock AI-powered insights, new revenue models, and better patient outcomes.



Chapter 1

The challenges to medical-grade connectivity



Connectivity is no longer a feature. It's the foundation of MedTech value

Most MedTech organisations already know the connected device opportunity is enormous. The harder question is why so many remain stuck between pilot and production. The answer: they underestimate the architectural complexity of implementing connectivity at sale.

A 2025 Deloitte survey (Deloitte, 2025) reveals the extent of the disconnect: MedTech executives see interoperability (45%) and data privacy (32%) as the top barriers to adoption, while healthcare providers point to demonstrating end-user value (32%) and budget constraints (27%). The industry isn't just facing technical challenges, it's facing alignment challenges.

Nine architectural challenges to medical device connectivity

Medical-grade connectivity isn't one problem, it's nine interconnected ones. Weakness in any single area cascades into others. The architectural challenge radar chart below visualises all nine and their dependencies. Together, these nine challenges define whether connectivity becomes a scalable growth platform or a stalled innovation initiative.

1. **Regulatory and compliance foundation.** Connected features often require separate regulatory submissions under the EU MDR, FDA QMSR, or IVDR. Adding cloud processing or AI analytics to an existing device can trigger reclassification. Cybersecurity controls must span the entire device lifecycle, not merely a one-time checkbox.
2. **Security architecture framework.** Connected medical devices are high-value cyber targets where a breach risks lives, not just data. Multi-layered security like device encryption, secure communications, hardware security modules, vulnerability management must be built in from day one. The European Cyber Resilience Act (CRA) makes manufacturers directly responsible for cybersecurity throughout a product's lifecycle.
3. **Cloud platform architecture.** Infrastructure must meet healthcare-grade compliance requirements, including encryption at rest and in transit, data residency, and strict access management, while also delivering high performance. This includes multi-protocol data ingestion, specialised time-series storage, and low-latency processing for critical alerts. Cloud architecture choices directly affect clinical safety.
4. **Device management and monitoring.** Secure OTA updates, full lifecycle management, and digital twins that reflect actual device state in real time. Intelligent alerting must distinguish a clinical emergency from a routine battery warning. As fleets scale from hundreds to thousands of devices, complexity grows exponentially.

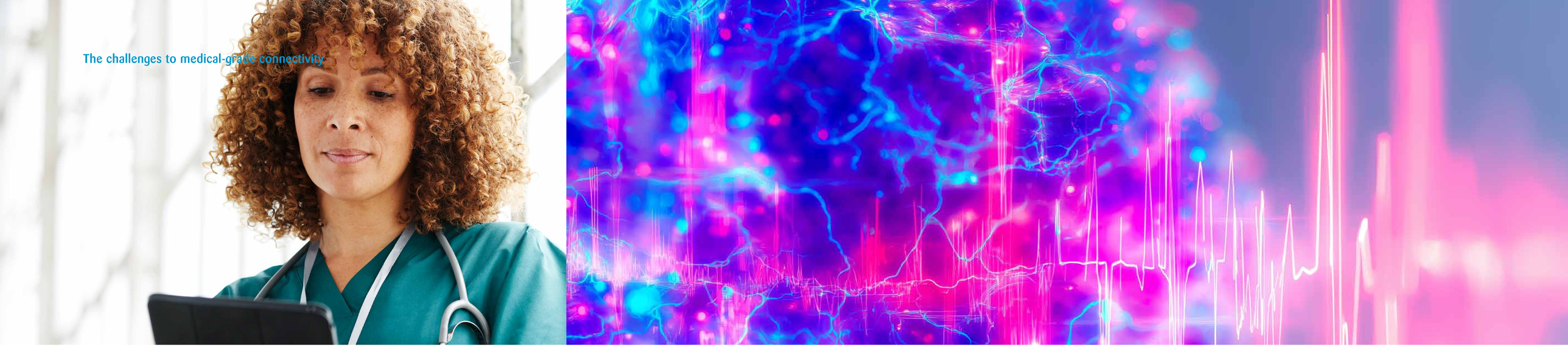
5. **Interoperability and standards.** Integration with EHRs, clinical workflows, and imaging systems requires compliance with HL7 FHIR, DICOM, and other standards. However, many devices still run proprietary protocols. Without interoperability, even the most advanced connected device sits in a data silo.

6. **Scalability and performance.** Systems must handle hundreds to millions of devices across geographies, network conditions, and infrastructure maturity levels, all with consistent performance. A cardiac monitor in a remote clinic must deliver the same reliability as one in a university hospital.

7. **Clinical integration and user experience.** Healthcare providers don't want another dashboard. Instead, they want data integrated into existing workflows. As devices move into patients' homes, they must also work for people with no medical training, limited mobility, or low digital literacy.

8. **Quality assurance and risk management.** Connected devices need testing environments that simulate real-world conditions, automated deployment pipelines with quality controls, and safe failure-handling. For instance, if a device loses connectivity mid-procedure, the system maintains operational safety. Traditional MedTech QA, designed for standalone hardware, often falls short here.

9. **Operational excellence.** Once a connected device is deployed, the work really begins. Incident response, performance monitoring, continuous evidence collection for audits, and predictive maintenance analytics all become core product functions. This is a fundamental shift from how most MedTech companies operate today.



These challenges don't exist in isolation

A security gap (challenge 2) becomes a regulatory failure (challenge 1). Poor interoperability (challenge 5) undermines clinical integration (challenge 7). Scaling without robust device management (challenge 4) creates QA complications (challenge 8).

These challenges are why connectivity programmes stall. The proof of concept works in controlled conditions. Under real-world conditions, regulators ask questions the architecture can't answer, security assessments reveal fundamental gaps, or the system collapses under real-world data volumes.

The regulatory baseline: control and traceability

Regardless of jurisdiction, every regulatory framework for connected medical devices ultimately centres on two requirements:

- **Control:** Every component – firmware, cloud infrastructure, data pipeline – must behave as intended, every time. In a connected ecosystem with continuous updates and third-party integrations, demonstrating this level of control is significantly more complex than for standalone devices.
- **Traceability:** An unbroken chain of evidence showing which software version ran on which device, what data was processed, how decisions were made, and what changed between any two points in time.

The EU MDR, FDA's Computer Software Assurance (CSA) framework and the Cyber Resilience Act all reinforce the expectation that devices are adapted for a world where 'the device' is no longer a self-contained object but a node in a larger system.

Organisations that build control and traceability into their architecture from day one will find the path to market smoother. Those that treat compliance as a bolt-on will face costly remediation, or lose market access entirely.

The opportunity behind the complexity

The complexity of medical-grade connectivity is precisely what makes it a durable advantage. Organisations that solve this will unlock predictive maintenance, real-time clinical insights, AI-powered decision support, and new service-based revenue models. The hurdles are real, but they're not insurmountable. What they require is an architecture-first approach that addresses all nine challenges as an integrated whole.

In Chapter 2, we'll show you exactly how to do that – with a step-by-step architectural flow built on AWS.

Chapter 2

Implementing medical-grade connectivity with AWS

From challenge to architecture: an eight-stage approach.

This chapter provides the solution to the architectural challenges described previously.

A proven, eight-stage architectural flow that addresses each of the nine challenges systematically. While this playbook demonstrates the approach on AWS, the architectural principles are cloud-agnostic.

This isn't a theoretical framework. It reflects how Zühlke designs and delivers connected medical device platforms for MedTech and healthcare organisations, combining deep healthcare domain expertise with hands-on AWS cloud engineering. Each stage maps to specific AWS services, chosen for their compliance capabilities, scalability, and fit in regulated healthcare environments.

The eight stages at a glance

The table below summarises the end-to-end data journey from the moment a device is turned on to ongoing compliance and exception handling.

End-to-End Value Stream Map

	What it achieves	Data flow	Key AWS services	Challenges
1 Initialise & Authenticate — Device	Zero-trust device identity via secure boot validation and cryptographic certificates	Device powers on → firmware integrity check → credential retrieval → mutual TLS to cloud	AWS IoT Core, AWS Private CA, AWS KMS, X.509 Certs	1, 2
2 Register & Configure — Device	Automated digital twin setup with configuration delivery and continuous security audit	Authenticated device → cloud registration → config push → clinical layer notified	IoT Device Shadow, IoT Device Defender, IoT Jobs	4, 9
3 Operational Data Flow — Edge	Low-latency telemetry with edge processing and store-and-forward resilience	Sensor data → edge processing & buffering → MQTT/TLS transmission → cloud ingestion	MQTT via IoT Core, IoT Greengrass, Kinesis Streams, API Gateway	3, 6, 8
4 Process & Store — Cloud	FHIR-compliant data storage with real-time streaming analytics and retention	Raw data → validate & transform to FHIR → time-series DB + data lake + clinical DB	HealthLake, Timestrea, Kinesis Analytics, S3 Data Lake	5
5 Integrate & Support — Cloud	AI-driven clinical insights pushed into EHR workflows with full explainability and audit trails	Processed data → FHIR API to EHR → real-time dashboards → AI/ML insights to clinicians	Bedrock, SageMaker, Comprehend Medical, API Gateway	7
6 Manage & Control — Cloud	Fleet-wide visibility with staged OTA updates, autorollback, and bidirectional device commands	Fleet monitoring → config push / OTA update → canary rollout → rollback if errors	IoT Device Mgmt, IoT Jobs, CodePipeline, CloudWatch	4
Cross-Cutting Concerns				
7 Comply & Audit — Compliance & Audit	Continuous automated compliance – every API call, config change & access event logged permanently	Every interaction → continuous compliance checks → noncompliance auto-flagged → auditready	CloudTrail, AWS Config, GuardDuty, Security Hub	1, 9
8 Handle & Recover — Exception Handling & Recovery& Audit	Multi-region resilience with offline operation – system may lose capability but never becomes unsafe	Failure detected → automatic failover → device continues offline → data reconciled on reconnect	AWS Backup, Route 53, IoT Greengrass, Auto Scaling	8

Cloud-Agnostic Principles

The architectural flow applies to any cloud platform. AWS services shown are the recommended implementation based on compliance capabilities, scalability, and healthcare-environment fit.

Control & Traceability

Every component must behave as intended, every time. An unbroken chain of evidence shows which software version ran on which device, what data was processed, and what changed.

Clinical Safety First

AI enhances clinical judgement, not replaces it. Every recommendation must be traceable and explainable. The system degrades gracefully – less capable without connectivity, but never unsafe.

Connecting medical device data on AWS

The following section provides essential technical context to brief your architecture team and evaluate implementation options. If you are approaching the problem from a strategic perspective, focus on how each stage reduces regulatory, operational, or cyber risk.

Stage 1: Device initialisation and authentication

Every connected device must establish a trusted identity before it transmits a single byte of data. This enables the zero-trust foundation for all subsequent controls.

- **Secure boot validation** ensures the device firmware hasn't been tampered with before it connects to any network.
- **X.509 certificate-based identity** via AWS IoT Core gives each device a unique, cryptographically verified identity - no shared keys or passwords.
- **Device credentials** are protected in secure hardware (TPM or secure element), while AWS Key Management Service (KMS) handles encryption key lifecycle, ensuring that secrets never leave secure hardware boundaries.

This stage directly addresses challenges 1 (regulatory compliance) and 2 (security architecture) from Chapter 1. Without reliable and secure device identity, downstream processes can't be relied upon.

Stage 2: Device registration and configuration

Once authenticated, each device needs to register itself and receive its configuration. This needs to be done automatically, at scale, and without manual intervention.

- **AWS IoT Device Shadow** creates a digital twin for each device: a cloud-based representation of its desired and reported state. This enables configuration management even when the device is intermittently connected.
- **Automated configuration delivery** ensures devices receive the correct firmware version, clinical parameters, and security policies for their specific deployment context.
- **AWS IoT Device Defender** continuously audits device configurations against security best practices, flagging drift before it becomes a compliance issue.

This stage lays the groundwork for challenge 4 (device management) and 9 (operational excellence) by establishing the control plane for your fleet.

Stage 3: Operational data flow

This stage is where the clinical value starts flowing: device telemetry such as vital signs and sensor readings, as well as diagnostic data, is transmitted securely.

- **MQTT protocol via AWS IoT Core** provides lightweight, reliable messaging optimised for constrained devices and variable network conditions.
- **AWS IoT Greengrass** enables edge processing for time-critical applications. Data that needs immediate action (e.g. a critical vital sign alert) is processed at the edge; everything else is streamed to the cloud for deeper analysis.

- **Local buffering and store-and-forward** ensures no data is lost during connectivity interruptions, which is critical for devices deployed in environments with unreliable networks.

This stage is where challenges 3 (cloud platform architecture), 6 (scalability), and 8 (exception handling) intersect. The architecture must handle variable data volumes while maintaining low latency for critical alerts.

Stage 4: Cloud data processing and storage

Raw device data becomes clinically meaningful information through validation, transformation, and compliant storage.

- **AWS HealthLake** provides FHIR-compliant data storage purpose-built for healthcare. It normalises data from different device types and makes it searchable using standard healthcare data models.
- **Amazon Timestream** handles high-volume time-series device data (sensor readings, telemetry) with automatic scaling and built-in data lifecycle management.
- **Amazon Kinesis** enables real-time streaming analytics – supporting anomaly detection, alert triggering and clinical dashboards as data arrives.

This stage addresses challenge 5 (interoperability) head-on by ensuring data is stored in line with industry standards from the outset, rather than retrofitted later.

Stage 5: Clinical integration and decision support

Connected device data only creates value when it reaches clinicians in a form they can act on, integrated into existing workflows and not siloed in yet another dashboard.

- **EHR synchronisation** via FHIR APIs pushes device-generated insights directly into electronic health records, where clinicians already work.
- **Amazon Bedrock** enables generative AI for tasks such as summarising patient trends and flagging risk patterns, without compromising data boundaries or explainability.
- **Amazon SageMaker** supports custom ML models for clinical decision support, with built-in model versioning and audit trails essential for regulated AI.

This is where challenge 7 (clinical integration and UX) meets the AI opportunity. The key principle: AI should enhance clinical judgement, not replace it, and every recommendation must be traceable and explainable.

Stage 6: Device management and control

Managing a fleet of connected medical devices in production is fundamentally different from managing traditional IT assets. Updates must be safe, staged, and reversible.

- **AWS IoT Device Management** provides fleet-wide visibility: which devices are online, which firmware version they're running, and what their health status is.
- **AWS IoT Jobs** orchestrates secure OTA updates with configurable rollout strategies like canary deployments, percentage-based rollouts, and automatic rollback if error rates exceed thresholds.
- **Bidirectional command and control** enables remote configuration changes and, where clinically appropriate, remote device adjustments, which are all logged and auditable.

For regulated devices, every update is a potential re-validation event. The architecture must make updates safe and traceable by default, not as an afterthought.

Stage 7: Compliance and audit

In a connected device ecosystem, compliance isn't a periodic activity, it's a continuous, automated process.

- **AWS CloudTrail** logs every API call and configuration change across your entire AWS environment, creating a permanent audit trail.
- **AWS Config** continuously evaluates your infrastructure against compliance rules, automatically flagging non-compliant resources and reducing the need for manual audits.
- **Amazon GuardDuty** provides intelligent threat detection, monitoring for malicious activity and unauthorised behaviour across your AWS cloud infrastructure, while **AWS IoT Device Defender** tracks device-side security metrics and anomalous device behaviour

This stage is the technical implementation of the 'control and traceability' principle from Chapter 1. It transforms compliance from a documentation burden into an automated, always-on capability - aligning with both the FDA's Computer Software Assurance (CSA) approach and the EU Cyber Resilience Act's continuous monitoring expectations.

Stage 8: Exception handling and recovery

Medical-grade systems must be designed for failure. It's impossible to prevent failure entirely, but when it occurs it must be handled safely and predictably.

- **Multi-AZ and multi-region deployment patterns** provide resilience against regional outages, keeping your connected device infrastructure operational.
- **AWS Backup** with cross-region replication protects clinical data against data loss scenarios.
- **Offline operation and sync** capabilities (built in stage 3 via Greengrass) ensure devices continue to function safely when cloud connectivity is interrupted, then reconcile data when the connection is restored.
- **Amazon Route 53 health checks** enable automatic failover to healthy endpoints, minimising downtime for clinical-facing services.

This stage directly tackles challenge 8 (QA and risk management). The goal is controlled degradation: the system may get less capable without connectivity, but never unsafe.

Architecture is only half the picture

These eight stages provide a robust technical blueprint. But technology alone doesn't deliver medical-grade connectivity. The organisations that succeed are the ones that also transform how they work: breaking down silos between R&D, quality, and IT; shifting from periodic audits to continuous validation; and building the cloud expertise needed to operate these platforms long-term.

That's what Chapter 3 addresses: preparing your organisation for the connected future.

Chapter 3

Preparing the organisation

Technology is only half the transformation

In Zühlke's experience, the most common reasons connectivity programmes stall aren't technical, they're organisational. Teams work in silos, compliance processes haven't been designed for continuous delivery, and the cloud expertise needed to operate these platforms doesn't yet exist in-house. This chapter addresses the three organisational shifts that are as critical as the architecture itself.

1. Breaking silos: from 'hardware-first' to 'platform-first'

Most MedTech organisations are still structured around hardware product lines. R&D designs the device, then hands it off to IT for connectivity and to the quality assurance department for compliance. This process works for standalone devices, but falls short for connected ones.

Medical-grade connectivity requires cross-functional teams from day one. Firmware, cloud, security, and regulatory departments need to work together, not sequentially. It requires shifting KPIs from 'devices shipped' to 'patient outcomes enabled' or 'uptime delivered'. And it requires treating devices as endpoints in a larger ecosystem, not standalone products.

The silo-breaker matrix below visualises where R&D, IT and quality assurance must collaborate at each project phase, from discovery through to post-market operations. The critical insight: there is no phase where any single function can operate independently.

Phase 1: Discovery (Weeks 1 – 4)

Goal: Align stakeholders, select use case, assess regulatory impact

Function	Activities	Collaboration Points
R&D /Engineering	Define device connectivity requirements | Map firmware vs.cloud-updatable logic | Identify sensor data flows & edge processing needs	Joint architecture assessment with IT; regulatory impact review with QA
IT / Cloud & Security	Evaluate cloud platform (AWS) fit | Assess currentinfrastructure & skills gaps | Define security architecture principles	Co-design eight-stage flow with R&D; compliance scoping withQA
Quality & Regulatory	Determine classification impact of connectivity | Engage notified body/ regulatory pathway early | Define validation strategy for conn. features	Align success criteria with R&D; review cloud compliance with IT

Phase 2: Alpha / MVP (Weeks 5 – 10)

Goal: Build core architectural flow, establish compliance foundations

Function	Activities	Collaboration Points
R&D / Engineering	Implement device authentication (Stage 1) | Build datatransmission pipeline (Stage 3) | Develop edge processing & local buffering	Integrate with cloud services builtby IT; feed test artefacts to QA
IT / Cloud & Security	Deploy IoT Core, Device Shadow | Greengrass | Set upCloudTrail, AWS Config from day one | Build CI/CD pipeline with compliance guardrails	Provide device registration APIs to R&D; automate audit logging for QA
Quality & Regulatory	Validate device-to-cloud data integrity | Establish automated evidence collection | Test with clinical users in realistic conditions	Define acceptance criteria with R&D; verify audit trails built by IT

Practically, this means establishing cross-functional 'product platform' teams, creating modular firmware architectures that separate hardware-specific code from cloud-updatable business logic, and building digital twins for simulation and testing. The organisational design must mirror the system architecture.

2. The continuous validation mindset

Traditional MedTech validation is built around periodic audits and static documentation. You validate once, lock down the system, and re-validate when something changes. This approach cannot keep pace with connected devices that receive regular software updates, process streaming data, and integrate with evolving cloud services.

The industry is catching up. The FDA's Computer Software Assurance (CSA) framework encourages risk-based, automated approaches to software validation. The EU Cyber Resilience Act (CRA) mandates continuous cybersecurity monitoring throughout a product's lifecycle. Both point in the same direction: compliance must become continuous and automated, not periodic and manual.

What this looks like in practice:

- **Validation as code:** Test scripts, compliance checks, and documentation generation are automated and version-controlled, not locked in Word documents.
- **Policy as code:** Compliance controls are built into infrastructure-as-code templates (e.g. via AWS Config), so every deployment is compliant by default.
- **Continuous evidence collection:** Audit trails, change logs, and validation artefacts are gathered automatically, ready for regulators at any time, not assembled retroactively.

Phase 3: Beta / Scale (Weeks 11 – 16)

Goal: Automate compliance, expand integration, add device types

Function	Activities	Collaboration Points
R&D / Engineering	Implement OTA update mechanism (Stage 6) | Buildclinical integration/ FHIR APIs (Stage 5) | Onboard additional device types to platform	Coordinate rollout strategies with IT; validate updates with QA
IT / Cloud & Security	Move to policy-as-code & validation-as-code | Implement multi-region resilience (Stage 8) | Scale CCoE: self-service tooling & golden paths	Provide platform patterns to R&D; automate compliance checks for QA
Quality & Regulatory	Continuous validation of deployment pipeline | Adapt for new regulatory jurisdictions | Verify AI/ML model audittrails (Stage 5)	Review OTA processes with R&D; consume automated evidence from IT

Phase 4: Live / Operate (Ongoing)

Goal: Post-market surveillance, continuous validation, fleet management

Function	Activities	Collaboration Points
R&D /Engineering	Predictive maintenance analytics | Firmware lifecycle management | New feature development & device iterations	Coordinate safe updates with IT; provide post-market data to QA
IT / Cloud & Security	Fleet monitoring & incident response | Continuous threat detection (GuardDuty) | Performance optimisation & cost management	Support R&D deployments; maintain always-on compliance for QA
Quality & Regulatory	Post-market surveillance & reporting | Continuous evidence collection for audits | Re-validation for significant changes	Review field data with R&D; audit infrastructure changes with IT

Cross-Functional Dependencies

Why This Matters: A security gap (R&D) becomes a regulatory failure (QA). Poor interoperability (R&D) undermines clinical integration (IT). Scaling without robust device management (IT) creates QA complications. These cascading dependencies are why connectivity programmes stall — and why cross-functional collaboration at every phase is non-negotiable.

Dependency	Description
R&D ↔ IT	Device requirements shape cloud architecture; firmware updates flow through CI/CD pipelines
IT ↔ QA	Automated compliance infrastructure replaces manual audits; always-on evidence collection
QA ↔ R&D	Validation criteria inform design choices; post-market data drives device iterations

- **Compliance guardrails in CI/CD pipelines**: Security scanning, traceability verification, and automated GDPR/HIPAA checks run on every deployment so issues are caught before they reach production.

The goal is to make compliance easier than non-compliance. When the 'golden path' through your deployment pipeline is also the compliant path, teams move faster and regulators receive stronger evidence.

3. Closing the skills gap: the Cloud Centre of Excellence

Very few engineers understand both medical device regulations and cloud-native architecture. This uncommon combination of expertise is exactly what connected device programmes require, and it's the biggest skills gap most MedTech organisations face.

The proven solution is a Cloud Centre of Excellence (CCoE), and the data confirms this. According to AWS, 83% of organisations with a CCoE report it as effective, citing reduced security risks, lower costs, and improved agility (AWS, 2023). In regulated industries specifically, mature CCoEs are associated with 25% lower cloud operational costs and significantly faster time-to-market for new digital services (Betsol, 2024).

However, the model that is used matters. A CCoE that becomes a bottleneck, requiring approval for every deployment, centralising knowledge, creating ticket queues, defeats the purpose. The modern CCoE functions as a platform engineering team that makes it easy for product teams to move fast and stay compliant:

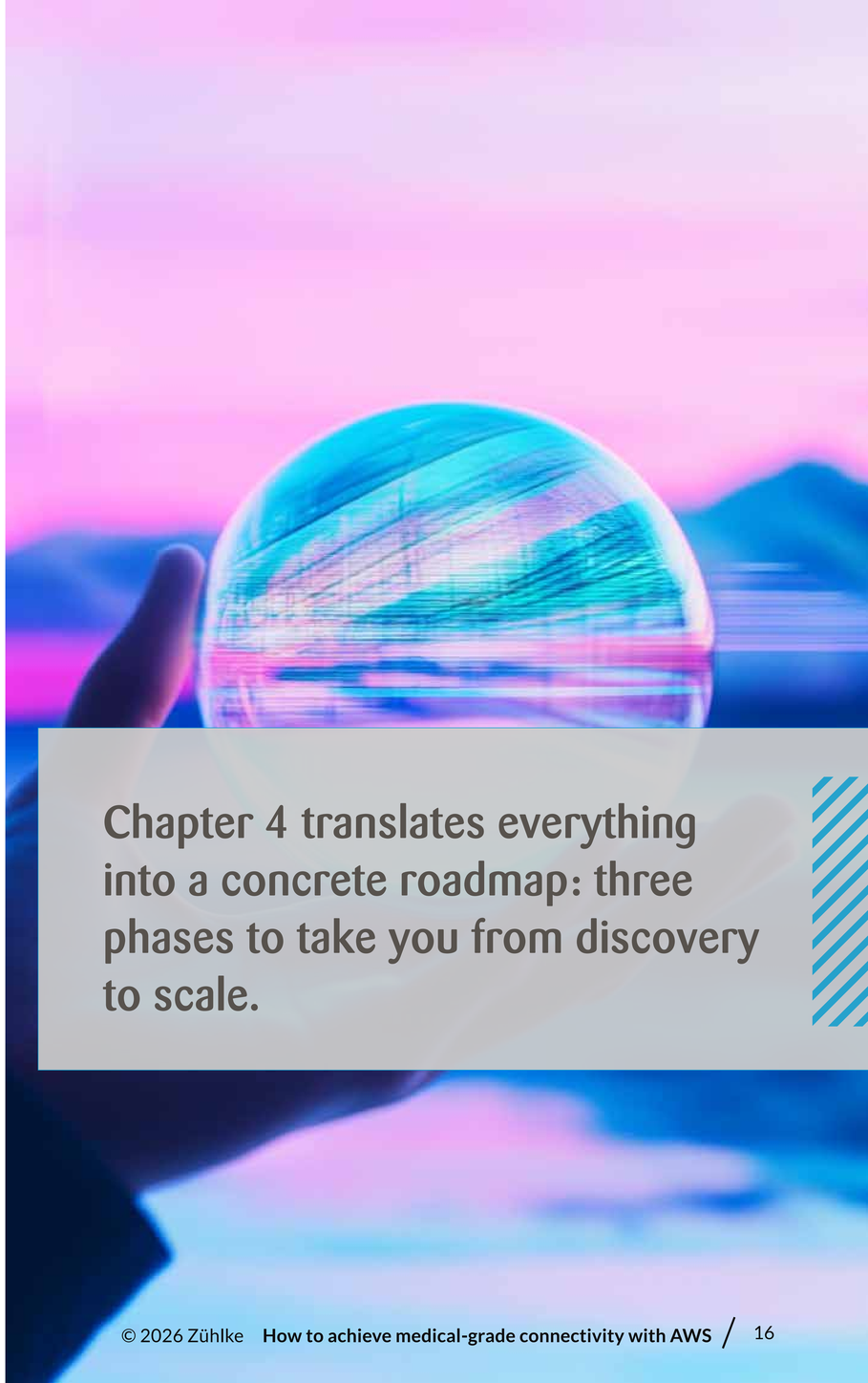
- **80% platform**: Build self-service cloud infrastructure with pre-approved, compliance-ready patterns. Automate security, validation, and deployment. Provide 'golden paths' that are easier to use than going rogue.

- **20% enablement:** Temporary embedded support to upskill product teams. Knowledge transfer, not knowledge hoarding. The CCoE's effectiveness is measured by how well it distributes cloud competence across the organisation.

For MedTech specifically, a well-designed CCoE concentrates the rare regulatory-plus-cloud expertise and makes it accessible: translating MDR and FDA requirements into reusable technical patterns, automating SBOM generation and vulnerability scanning, and providing pre-validated architectures for common device classes. Zühlke works with organisations to stand up exactly this kind of capability - often starting as an external enabling team that builds the internal platform and transfers knowledge progressively.

Bringing it together

Breaking silos, automating compliance, and building cloud expertise aren't optional extras - they're essential. Without them, even the best architecture will stall in implementation. The organisations that move fastest are the ones that tackle the technical and organisational transformation in parallel, not sequentially.



Chapter 4

The roadmap

From strategy to production in three phases

This chapter turns strategy into a concrete, phased plan. The industry is already proving this works. MedTech companies using purpose-built connected device platforms on AWS have cut time-to-market by up to 80% compared to building cloud infrastructure from scratch. This has been achieved by starting with validated, compliance-ready building blocks and scaling from there.

Phase 1: Discovery (weeks 1 – 4)

Goal: Identify your first medical-grade connectivity use case and validate that the approach works for your organisation.

Start with a single, well-scoped use case, not an enterprise-wide transformation. The best candidates are devices that already generate clinical data but transmit it manually or not at all: remote monitoring devices, diagnostic equipment that stores results locally, or devices where connectivity would unlock a clear clinical or operational improvement.

Key activities:

- **Stakeholder alignment**. Bring R&D, IT, quality assurance and regulatory teams together to agree on the use case, success criteria, and risk appetite.
- **Architecture assessment**. Map the selected use case against the eight-stage architectural flow (Chapter 2). Identify which stages are critical for the MVP and which can follow later.
- **Regulatory scoping.** Determine the classification impact of adding connectivity. Engage your notified body or regulatory pathway early, not after the architecture is built.
- **Skills and gap analysis.** Assess your team's cloud and security capabilities. Define where you need external expertise (e.g. a partner like Zühlke) and where you'll build internally.

Outcome: A validated use case, a prioritised architecture blueprint, and a clear view of the team and skills needed to deliver the MVP.

Phase 2: MVP (weeks 5 – 10)

Goal: Build the core architectural flow on AWS for your selected use case from device to clinical integration.

The MVP should cover the full data journey, not just one piece. Even if it's a single device type and a limited user group, the architecture should implement all eight stages at a basic level. This avoids the common pitfall of building a demo that can't scale because foundational stages of security, compliance and exception handling were glossed over.

Key activities:

- **Implement the core flow.** Device authentication (stage 1), registration (stage 2), data transmission (stage 3), and cloud processing (stage 4) form the backbone and need to be built first.
- **Establish compliance foundations.** Set up CloudTrail, AWS Config, and automated audit logging (stage 7) from day one, not as a post-build addition. This is what differentiates a demo from a medical-grade MVP.
- **Clinical validation.** Test with actual clinical users in realistic conditions. Make sure that data is available to the right people in a form they can act on.

- **Stand up the CCoE seed team**. Begin building internal cloud expertise in parallel (Chapter 3). Even a small core team of two to three people who deeply understand the platform will accelerate the process.

Outcome: A working, compliant connected device pipeline on AWS. It will be limited in scope, but architecturally sound and ready to scale.

Phase 3: Scale (weeks 11+)

Goal: Automate compliance, expand clinical integration, and scale to additional device types and markets.

With the core architecture proven, the focus shifts from 'does it work?' to 'does it scale safely?' This is where continuous validation, automated compliance, and the CCoE (Chapter 3) become essential.

Key activities:

- **Automate everything.** Move from manual compliance checks to policy-as-code. Implement 'validation as code' pipelines so every deployment is automatically tested, documented, and audit-ready.
- **Expand clinical integration.** Connect to EHR systems via FHIR APIs (stage 5). Introduce AI-powered decision support where clinically appropriate.
- **Add device types and markets.** Onboard additional devices to the platform. Adapt for new regulatory jurisdictions as needed.
- **Mature the CCoE.** Transition from external enablement to internal capability. Build self-service tooling and 'golden paths' that make it easy for new teams to build on the platform.

Outcome: A scalable, multi-device connected care platform with automated compliance, and the internal capability to operate and extend it.

The 90-day quick-start timeline

The table below provides a week-by-week overview of key milestones across all three phases - designed to give C-level sponsors clear visibility into progress and decision points.

Timeframe	Key activity	Milestone / deliverable
Phase 1: Discovery		
Week 1–2	Stakeholder alignment and use case selection	Agreed use case and success criteria
Week 2–3	Architecture assessment against eight-stage flow	Prioritised architecture blueprint
Week 3–4	Regulatory scoping and skills gap analysis	Classification impact report; team plan
Phase 2: MVP		
Week 5–6	Core flow implementation (stages 1 – 4)	Device-to-cloud data pipeline live
Week 7–8	Compliance foundations and audit logging (stage 7)	Automated audit trail operational
Week 9–10	Clinical validation and user testing	Validated MVP; clinical feedback integrated
Phase 3: Scale		
Week 11–12	Automate compliance pipelines (policy-as-code)	Fully automated deployment pipeline
Week 12+	Expand to additional devices, markets, & AI use cases	Scalable multi-device platform

Start the conversation

Medical-grade connectivity is complex, but not unachievable. The key is to start with a focused use case, build on a proven architectural foundation, and scale deliberately.

Zühlke partners with MedTech organisations across Europe and Asia to make this journey faster, safer, and more predictable. We help take companies from initial discovery through to production-ready, compliant connected device platforms on AWS.

Ready to take the first step? Let's explore how these principles apply to your specific devices, regulatory landscape, and organisational setup. Contact our connected health team to schedule a discovery session.

Ronnie Bose
Group Head Devices & Chief Technology Officer Health & Partner
ronnie.bose@zuehlke.com

Mihai Popa
Lead Cloud Architect
mihai.popa@zuehlke.com

About Zühlke

Zühlke is a global transformation partner, with engineering and innovation in our DNA. We're trusted to help clients envision and build their businesses for the future – to run smarter today while adapting for tomorrow's markets, customers, and communities.

Our multidisciplinary teams specialise in tech strategy and business innovation, digital solutions and applications, and device and systems engineering. We excel in complex, regulated spaces including health and finance, connecting strategy, tech implementation, and operational services to help clients become more effective, resilient businesses.

Founded in Switzerland in 1968, Zühlke is owned by its partners and located across Europe and Asia. Our venture capital arm, Zühlke Ventures, provides start-up financing in HealthTech.

zühlke
empowering ideas

Published by

Zühlke Engineering AG
Zürcherstraße 39J
8952 Schlieren (Zürich)
Switzerland

info@zuehlke.com
www.zuehlke.com

Image sources:
Getty image: cover, p.4, p.6, p.7, p.8, p.12, p.13,
AI-generated by Zühlke: cover, p.6, p.7, p.8, p.12, p.13, p.16, p.17, p.21