System Boundaries:
Who Controls What

Medical device security covers far more than the physical device. It covers the entire connected system: device, companion app, cloud backend, APIs, and clinical integrations. Defining boundaries early prevents late-stage disputes, procurement confusion, and gaps in your threat model.

Component	Your Security Responsibilities	Customer/ Hospital Responsibilities
1 **Device / Firmware**	Hardening, secure communications, device identity, secure update mechanisms (signing and rollback), tamper considerations (risk-based).	Physical security of device, network segmentation.
2 **Mobile App**	Authentication/authorisation flows, secure local storage, API request integrity, session management, security-relevant logging.	Device OS updates, application installation, user access governance.
3 **Cloud / Backend**	Tenancy isolation, secrets management, encryption boundaries, audit logging, infrastructure-as-code controls, vulnerability scanning (images/ dependencies).	Network firewall rules (if private cloud), user identity management integration.
4 **Integrations (EHR, APIs)**	Supported configurations documented, minimum TLS/auth requirements, API security standards, integration testing scope.	Network controls (firewalls, VPNs), identity governance, endpoint protection, access provisioning/deprovisioning.
5 **Shared Responsibilities**	Vulnerability intake process, incident response co-ordination, patch communications, evidence maintenance.	Reporting suspected incidents, applying patches within agreed timeframes, reviewing security advisories.

Note: Include explicit assumptions in your documentation. For example, “customer manages network segmentation” and “shared responsibility for cloud applies (config, IAM, logging)”. Assumptions left undocumented become disputes.

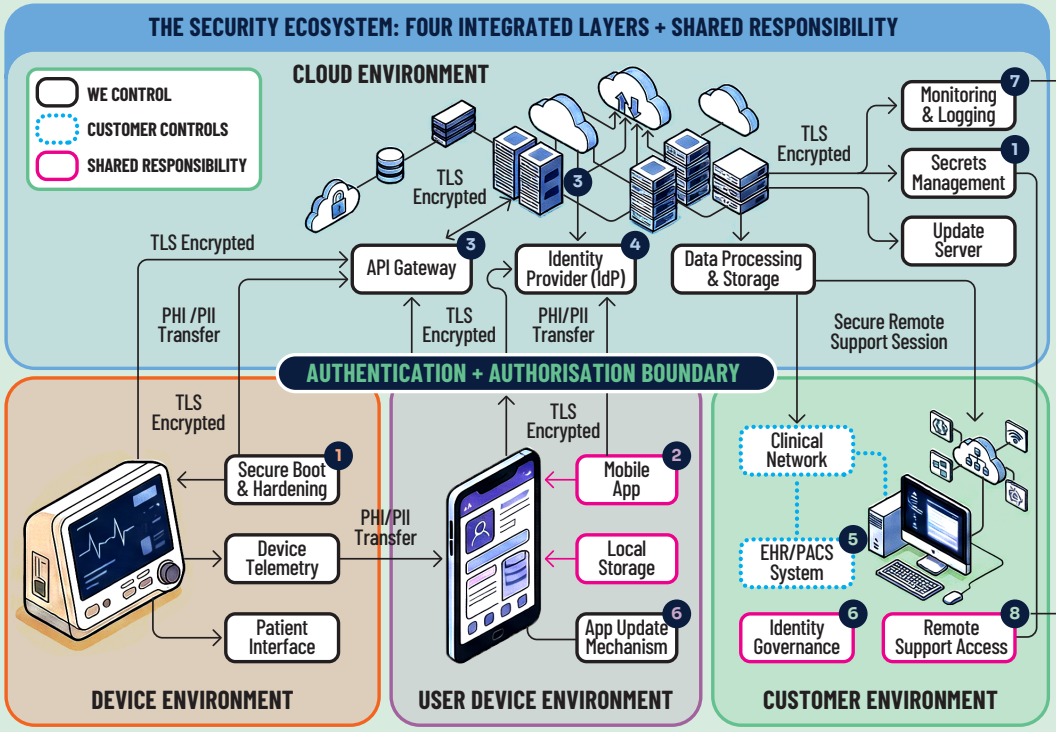
CYBER ALCHEMY®
ASSESS · PROTECT · ENABLE

CYBERALCHEMY.CO.UK

Bringing it to Life:
An Example System Boundary Diagram

CYBER ALCHEMY
ASSESS · PROTECT · ENABLE

MedTech Security:
End-to-End System Boundary and Services



Cyber Alchemy Consultancy Services

Technical Security Hardening

1 System hardening, 3 verification testing, penetration testing, and system architecture.

Clinical Access, Identity & Support Security

5 Identity governance, 6 IAM/PAM, SSO, privileged access, 8 secure remote support.

Lifecycle Security Engagement

2 Secure SDLC, CI/CD security, SBOM assurance, 4 compliance support, 7 vCISO guidance, and post-market security activities.

Data Table: Service Mapping

Service Area	Focus Highlights
Device, App & Endpoint Security	System hardening, secure update implementation, system verification testing plan development and execution.
Application, API & Cloud Security	AuthN/Z, Application, infrastructure and cloud penetration testing, cloud architecture hardening.
Identity, Access & Operational Security	IAM/PAM, SSO, secrets management, privileged access, secure remote support.
Threat Validation, Monitoring & Response	Red/purple teaming, adversary simulation, logging maturity, vulnerability assessment, and incident readiness.
Secure Delivery, DevSecOps & Training	Secure SDLC, CI/CD security, developer enablement training, SBOM assurance and awareness training.
Governance, Compliance & Post-Market Security	DTAC/EU MDR/ FDA510(k) compliance support, vCISO strategy, AI governance, and Cyber Essentials certification.