G-Cloud 15 (RM1557.15) MD Clone Ltd.

Infrastructure Software services

Service Definition

January 2026

MDCLONE

Table of contents

1 Introduction

1.1 Document structure

This Service Definition document explains the services offered by MDClone Ltd under the G-Cloud 15 Framework. It helps public sector buyers understand our service functionality, security, pricing, delivery approach and provides clear guidance on how to engage with us through the framework. The document is divided into the following sections:

- **Service description** – Outlines our Lot 2B Infrastructure Software services, including key features, benefits, delivery methodology and assurance measures such as security and compliance
- **G-Cloud alignment information** – Details how our services operate under the G-Cloud 15 framework, covering onboarding, service levels, data management, support and exit procedures
- **Security and data governance** – Explains our information security framework, encryption standards and business continuity measures
- **Supplier information** – Summarises our company background, mission, relevant experience and procurement routes
- **Pricing and commercial terms** – Provides clarity on pricing, invoicing and termination terms

1.2 How to use this document

- **For early-stage evaluation**, see **Section 2 (Service description)** for service scope, methodology and core benefits
- **For due diligence and contract preparation**, see **Section 3 (G-Cloud alignment information)** for onboarding, service levels, data management and exit processes
- **To assure compliance and data protection**, see **Section 4 (Security and data governance)** for our security framework and governance measures
- **For supplier verification**, see **Section 5 (Supplier information)** for company background, accreditations and procurement routes

2 Service description

2.1 About our service

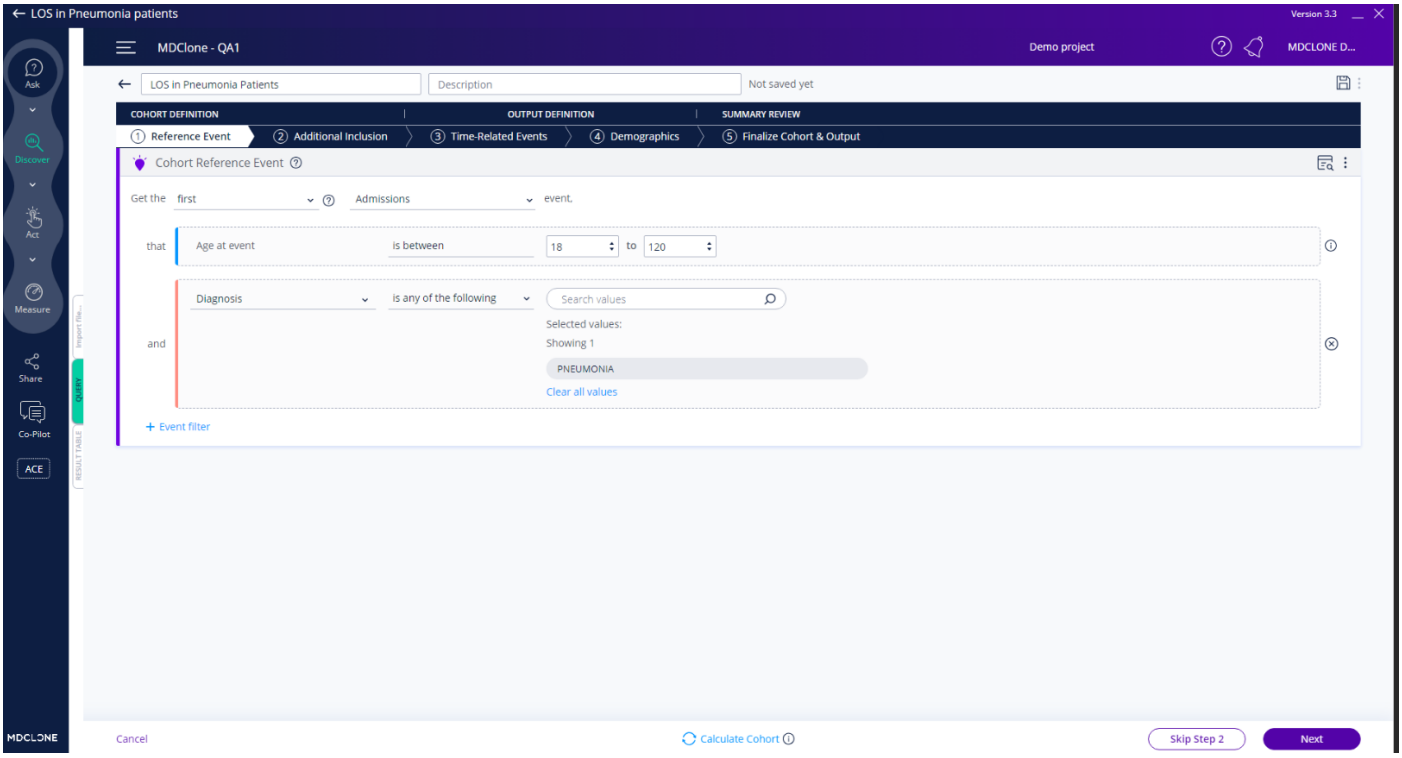
Introduction to the supplier and service context

MDClone was founded in 2016 and works with leading healthcare organisations worldwide, including NHS bodies and public sector partners. Our mission is to democratise healthcare data, enabling organisations to use their data safely, effectively and at scale to improve care, operations and research. We prioritise privacy and trust by design, applying secure-by-design and privacy-by-design principles in every engagement. We hold ISO/IEC 27001:2022 and ISO 27799:2016 certifications and comply with Cyber Essentials requirements for Lot 2B.

Service overview

The MDClone ADAMS Platform helps healthcare organisations unlock faster insights and measurable improvements by making data accessible, secure and actionable. Without relying on technical teams, it enables clinicians, managers and researchers to explore patient data safely and at scale. The platform combines self-service analytics, privacy-preserving synthetic data which is generated from source datasets but cannot be reversed to reveal the original data. It does not contain personal data and is used for testing, collaboration and early-stage exploration. It also uses an AI copilot to support natural language queries under strict governance. AI acts only as an assistive tool and supports, but does not replace, human judgment. AI does not make clinical or operational decisions. Users review and validate all AI outputs before taking action and AI operates within infrastructure that customers fully control. This approach removes bottlenecks, accelerates decision making and supports collaboration without exposing identifiable information.

ADAMS is designed for NHS Trusts, Integrated Care Boards and national programmes where local data remains controlled. It runs within client/customers/buyers 'private environment, reinforcing security and compliance with public sector standards. Requiring , access is browser-based, which reduces complexity and supports rapid adoption. Under G-Cloud 15 Lot 2B, our service provides infrastructure software capabilities and integration support aligned with government priorities for security, sustainability and cost efficiency.



Value and differentiators

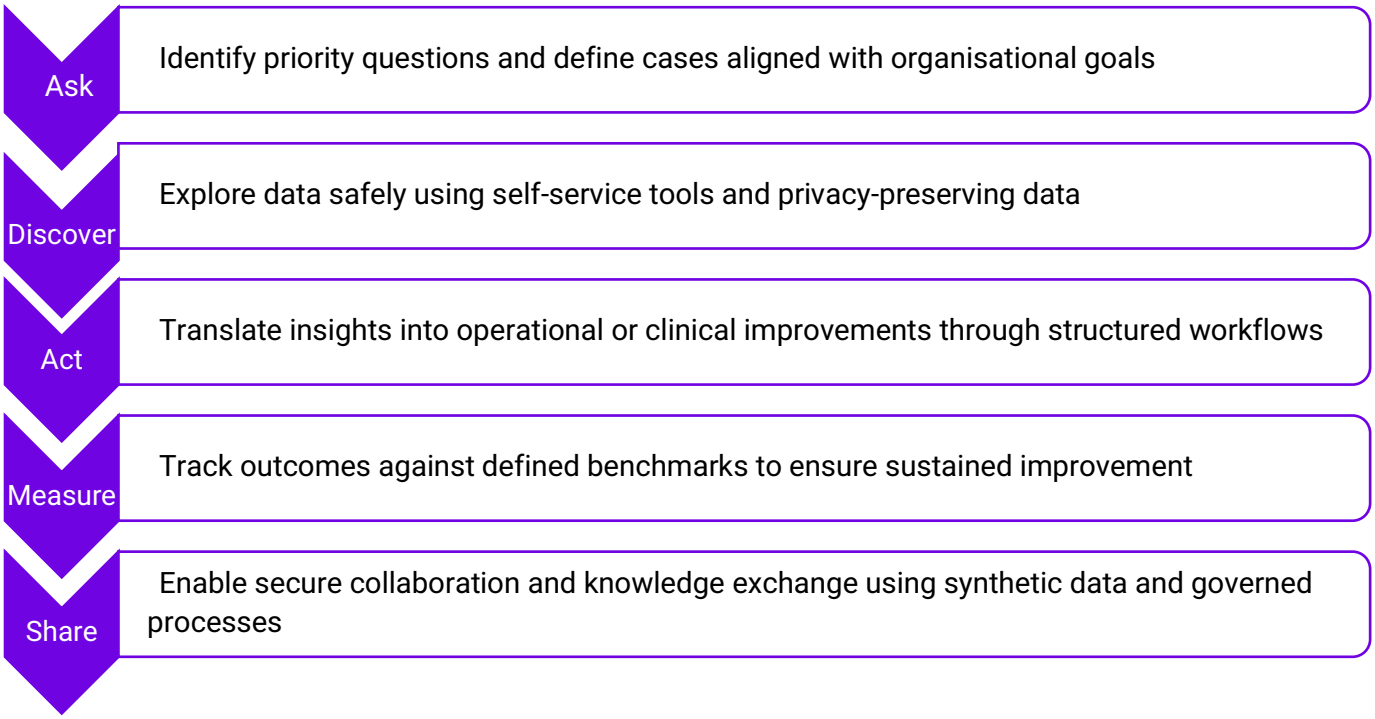
Our approach is distinctive because it combines privacy-led collaboration, self-service analytics for non-technical users and structured delivery through the ADAMS Centre methodology. It enables organisations to scale their data capabilities while ensuring safe and consistent use. The methodology also embeds both strong governance and sustainable adoption. By partnering with us, buyers gain a trusted delivery partner focused on outcomes, not just technology. We help you accelerate improvement cycles, reduce reliance on scarce technical resources and unlock the full value of your data.

Our key differentiators include:

- Privacy-preserving synthetic data for secure collaboration and research enablement
- Self-service access designed for clinicians and operational leaders
- AI-assisted exploration to accelerate insight generation under governance
- Support for structured and unstructured data, including natural language processing
- Proven delivery methodology that aligns with organisational priorities and governance requirements

2.2 Delivery framework

To ensure consistent, secure and outcome-driven delivery, we apply the **ADAMS Centre methodology**. This structured approach combines people, process and technology into a repeatable lifecycle that supports adoption and measurable impact. The methodology follows 5 stages: **Ask, Discover, Act, Measure and Share**.



Ensuring delivery is uniform, structured and successful, all consultants are trained in this methodology. Helping organisations scale data use safely and consistently, it embeds governance and adoption at every stage.

2.3 Service features / benefits

Our service delivers infrastructure software capabilities that enable secure, scalable and governed use of healthcare data within your private environment. Each feature addresses common public sector challenges and delivers measurable benefits.

Service features	Benefits
Self-service analytics enables clinicians, operational leaders and researchers to explore data directly without coding or reliance on technical teams.	Reduces delays caused by data silos and accelerates decision-making, improving productivity and responsiveness.
Privacy-preserving synthetic data Privacy-preserving synthetic data generates non-reversible datasets that mirror statistical properties of source data without containing identifiable information	Supports safe collaboration and research without breaching privacy or governance requirements, reducing compliance risk.
AI-assisted data exploration provides an optional AI copilot that supports natural language queries and pattern discovery under strict governance.	Simplifies complex analysis for non-technical users, speeding insight generation and reducing manual effort.
Support for structured and unstructured data includes natural language processing (NLP) capabilities to extract insights from clinical notes and other unstructured sources.	Expands the range of usable data, enabling richer analysis and more informed decisions.

Role-based access and governance implement configurable permissions aligned with organisational policies and information governance standards.	Maintains security and compliance while extending access to a wider range of roles.
Browser-based access delivers the platform through a secure web interface with no client-side installation required.	Simplifies deployment, reduces infrastructure overhead and supports rapid adoption.
Outcome measurement and benchmarking provide built-in tools to track improvements against defined targets and benchmarks.	Demonstrates impact transparently and supports continuous improvement.
Structured delivery through ADAMS Centre methodology follows a 5-stage lifecycle: Ask, Discover, Act, Measure and Share.	Ensures governance, adoption and repeatable success across all projects.

2.4 Service scope

Our service delivers infrastructure software for secure data access and exploration. It runs within your private environment and is accessed via a web browser. We align with Lot 2B scope for systems infrastructure software and deployment-centric platforms. Buyer-specific inclusions and exclusions will be confirmed in the Statement of Work (SoW).

2.4.1 Add-ons and extensions

You can extend the platform with optional components that increase flexibility and unlock additional value for your organisation:

- Private large language model (LLM) integration supports deployment of advanced AI features within your secure subnet, maintaining privacy and compliance while enabling innovation
- Additional training and advanced enablement services are available as chargeable options, giving your teams the knowledge and confidence to adopt the platform effectively and embed sustainable data use
- All add-ons are enabled only with your approval and governance and buyer-specific requirements will be confirmed in the SoW

2.4.2 Cloud deployment model

To maximise security and control, we deploy primarily as a private cloud within your environment.
This keeps compute and storage inside your secure perimeter and chosen region. To meet governance or interoperability needs, we also support a hybrid model. In hybrid mode, core components run privately while approved integrations use cloud adjacent services.

Default model: We safeguard sensitive healthcare data and we use a private cloud by default. Hybrid deployment options are available upon request and will be confirmed in the SoW.

Hosting location and data residency: Hosting occurs on premises or in your private cloud region as agreed. Data residency follows your organisational policy and remains under your control. This model reduces privacy risk and accelerates adoption as you retain control while unlocking faster access to trusted data.

2.4.3 Service constraints

Constraint	Description	Mitigation
Planned maintenance	Minor releases usually require no downtime. Major releases may require limited downtime.	Schedule outside business hours where possible. Provide advance notice as per the SoW.
Business hours	Standard hours are 09:00–17:00, Monday–Friday, excluding UK public holidays.	Arrange out of hours support for critical incidents by agreement.
Access to people and systems	Timely access to systems and subject matter experts is required.	Plan regular working sessions. Track decisions through project governance.
Third-party dependencies	Integrations may rely on approved application programming interfaces (APIs) or webhooks.	Enable only under buyer governance. Document dependencies in the SoW.
Optional private LLM	Azure or Amazon Web Services instances may be required for AI copilot features.	Isolate connectivity via site-to-site virtual private network (VPN). Confirm scope in design.
Productivity integrations	Licences for suites such as Microsoft 365 may be required.	Confirm licence ownership and scope before configuration.
Capacity and scale	Final sizing depends on data volume and workload.	Perform sizing during design. Reassess as usage grows.

2.4.4 System requirements

Category	Requirement
Supported browsers	Latest Google Chrome and Microsoft Edge.
Operating systems	Windows 10 and above. macOS 12 and above.
Mobile access	The platform is not designed for mobile devices.
Connectivity	Stable broadband connection. Recommended minimum bandwidth is 10-20Mbps for end-user browser access only. ETL ingestion and Kubernetes–Cloudera traffic run within the private deployment and are sized separately. (10 Gbps).
Deployment perimeter	Deployment occurs behind your firewall in your private environment.
Support access	A dedicated MDClone Administration Server (jump box) is required.

Network paths	Secure Shell (SSH) and Remote Desktop Protocol (RDP) must be open between the jump box and platform clusters.
Identity and access	Single sign on (SSO) is supported via Security Assertion Markup Language (SAML). Role based access controls will align with your governance.
Data ingestion	Secure connectivity to approved databases and file sources is required. A dedicated server manages extract, transform and load tasks.
Third party prerequisites	A SAML capable Identity Provider is required for SSO. Private LLM instance is optional for AI copilot.
Hosting and hardware	On premises or private cloud deployment in your selected region. No specialist client hardware is required.

2.7 Reselling

We do not resell any third-party cloud platforms or services, however, certain third parties must hold licenses for software such as Talend and Cloudera. As well as this, services are delivered exclusively by MDClone. This approach ensures full accountability for service quality, security, and compliance. Buyers benefit from a trusted provider with direct control over delivery and support.

2.8 User support

To help buyers maintain continuity and resolve issues quickly, we provide a structured and responsive support service. Our model is designed to reduce downtime and ensure smooth operations.
We align our support approach with recognised best practices and deliver it through a combination of self-service resources and a dedicated helpdesk. Escalation pathways ensure that complex issues reach technical specialists without delay.

2.8.1 Support details

Support features	Details
Channels	Buyers can contact us through email and an online ticketing portal. We do not provide phone or web chat support.
Hours	Standard support is available Monday to Friday, 08:00–17:00 (UK time). Ticket submission is available 24/7.
Accessibility standards	Our online ticketing portal meets WCAG 2.2 AA accessibility standards.
Response times	We aim to respond within four working hours for standard issues and within one working hour for high-priority incidents.
Support for third parties	Authorised third-party contractors can access support channels if approved by the buyer.
AI-driven support	We do not currently provide AI-driven self-service tools or chatbots.
Escalation process	Escalation is managed through the ticketing system. Critical issues are assigned to senior engineers immediately.
Account management	Each customer has a dedicated Account Manager who acts as the primary point of contact for strategic and operational needs.

2.8.2 Accessibility and usability

To ensure every user can access and use the service effectively, we design all interfaces and documentation to meet recognised accessibility standards. This approach supports adoption across the public sector without additional adjustments.

Our platform interface complies with the WCAG 2.2 AA and EN 301 549 standards. These standards ensure compatibility with assistive technologies such as screen readers and keyboard navigation tools.
We embed accessibility into our user-centred design process. During development, we test usability and accessibility with representative user groups and continuously review feedback. This iterative approach allows us to identify barriers early and implement improvements before release.

Enabling users to log and track support requests easily, our online ticketing portal also meets WCAG 2.2 AA standards. Documentation is available in accessible HTML and PDF formats. If required, to meet specific needs, Buyers can request alternative formats. We maintain accessibility by applying structured templates, clear language and consistent navigation across all materials. We ensure accessibility is a continuous commitment to usability for all users by combining compliance with proactive feedback loops.

2.9 How users benefit from working with our service

2.9.1 Browsers

Work faster with secure, browser-based access. The service supports modern “evergreen” browsers, including Google Chrome and Microsoft Edge. Using a supported browser, users can access the platform

from Windows, macOS or Linux devices. To use all features, JavaScript and cookies should be enabled. For transparency, we notify buyers before any change to supported browsers.

2.9.2 Desktop application

A dedicated desktop application is not required, which speeds up onboarding. Administrators manage the service through a secure web interface. Central device-management tools are not needed for end-user access.

2.9.3 Mobile

Protect focus and usability for complex analysis tasks on larger screens. The service is not designed for use on mobile devices. Users should access the platform on desktop or laptop browsers for best results. Mobile application support is not provided.

2.9.4 Service interface

Empower teams with a clear, role-based web experience that accelerates insight. The interface is fully web-based and uses configurable roles and permissions. SSO through Security Assertion Markup Language (SAML) is available where required. Helping users progress from question to result, dashboards undertake searches and task-oriented views provide valuable assistance. An administrator portal supports user management, password policies and platform maintenance. The interface supports self-service exploration, reusable queries and controlled export of approved outputs. Where enabled, natural language processing (NLP) supports analysis of unstructured clinical text.

2.9.5 API

Unlock integration flexibility with our secure Application Programming Interface (API). The API enables organisations to automate workflows and extend platform capabilities without manual intervention.
We provide a private API designed for controlled access within your secure environment. Through the API, users can manage configuration, trigger data onboarding processes, and export approved outputs for collaboration. The API supports integration with enterprise authentication, including Single Sign-On (SSO) via Security Assertion Markup Language (SAML). Comprehensive documentation is available in HTML and PDF formats.

2.9.6 Accessibility and usability

By driving adoption, reducing risk and improving outcomes for every user, we embed accessibility into our platform, helping organisations meet compliance obligations and deliver better experiences for staff and patients. To make every interaction simple and inclusive, we design our user interface (UI) and user experience (UX) for clarity and confidence. This ensures all users can work effectively without barriers.
We follow the Web Content Accessibility Guidelines (WCAG) 2.2 level AA and the UK Public Sector Bodies Accessibility Regulations. Complying with these standards supports equitable access. To reduce cognitive

load, we build predictable layouts and clear navigation. Keyboard navigation works across all features, with logical focus order and visible focus states. Skip links allow quick movement to main content.

To support users with visual impairments, colour contrast meets WCAG thresholds. Ensuring assistive technologies can interpret roles, names and states correctly, we use semantic HTML and Accessible Rich Internet Applications (ARIA) patterns where needed.

We test with screen readers, magnifiers and other assistive technologies across supported browsers. Testing combines automated checks, expert reviews and research with users who rely on accessibility features.

Before major releases, we apply accessibility checks throughout development. Our process includes WCAG-based checklists and continuous improvement cycles. To ensure interoperability and inclusive design, we also follow the government Open Standards Principles and to enhance usability over time, we invite and act on feedback from customers.

2.9.7 Customisation

Configurable design empowers organisations to scale data use without complexity. This supports faster adoption, consistent governance and measurable impact across clinical, operational and research workflows. To help you adapt the platform to local priorities without custom coding, we provide flexible configuration options that keep control in your hands.

To align with governance and operational processes, Administrators can configure user roles, permissions and workflow rules. To match your internal escalation paths, we can adjust your notification settings and approval routes. Focusing on the metrics that matter most to your teams, we can customise dashboards, reports and data fields. Offering a seamless solution, most configuration changes can be made directly by buyer administrators through an intuitive interface. For advanced options or complex scenarios, our technical team provides expert support to ensure safe and efficient implementation. This approach reduces reliance on bespoke development, accelerates deployment and ensures the platform remains aligned with your evolving needs.

2.9.8 Service levels and availability

The following service level agreements (SLAs) define the availability, responsiveness and performance standards for the MDClone ADAMS Platform under G-Cloud 15 Lot 2B. These commitments help your teams move from question to insight faster with clear expectations and rapid support.

We monitor performance through our support portal and platform monitoring capabilities. To drive action and improvement, we review results in structured service reviews. Any SLA breach triggers escalation, corrective actions and where agreed, service credits under the call-off.

We maintain these SLAs with proactive platform monitoring, a tiered incident process and focused service reviews. Our model empowers your teams while keeping privacy, security and governance in clear focus.

The platform is deployed within your secure infrastructure. Infrastructure availability and disaster recovery targets are determined by your policies and capabilities. We set any application-level availability target with you at call-off.

The ADAMS Platform is fully customer-hosted. All data storage and processing occur within your private infrastructure. As a result, infrastructure availability, RPO and RTO are governed by your controls. We align our software support SLAs to complement your resilience posture.

Standard service levels

Metric	Target	How we measure and report this
Ticket submission availability	24/7 ticket submission via the customer support portal	Submission timestamps in the portal. Reporting in service reviews
Support hours of service	Responses during business days, 09:00–17:00, customer local time	Support system timestamps. Reporting in service reviews
Priority 1 (P1) initial response time	Response within 4 working hours	Portal timestamps from ticket creation to first response
Priority 1 (P1) resolution or workaround	Resolution or workaround within 48 working hours	Portal timestamps from ticket creation to resolution or workaround
Priority 2 (P2) response time	Critical – production use is severely impacted and cannot reasonably continue – begin work within 8 working hours. Aim to resolve within 96 working hours.	Portal timestamps. Reported in service reviews
Priority 2 (P2) resolution	High – important features are unavailable with no workaround, materially impacting productivity. Initial response within 24 working hours.	
Priority 3 (P3) response time	Medium – important standard features are unavailable (workaround exists) or less significant features are unavailable (no reasonable workaround. Initial response within 48 hours.	
	Low – request for information, enhancement or documentation	

	clarification with no impact on platform operation. Clarification within 10 Business days.	
Out-of-hours support for critical incidents	Reasonable-effort support for critical incidents or pre-agreed activities	Incident logs and post-incident reviews
Planned maintenance notification	Scheduled outside business hours where possible. Advance notice provided	Change records and maintenance communications
Application availability (buyer-hosted)	Monthly availability target agreed at call-off	Buyer monitoring or agreed tooling. Reported in service reviews

Incident prioritisation and escalation process

To protect service continuity, we prioritise incidents based on impact and urgency. For transparency, all tickets are triaged in our support portal. Critical issues are immediately escalated to senior engineering and specialist teams. Management-level escalation applies for prolonged or high-impact incidents. To drive improvement, we complete root cause analysis and share a post-incident review for every major event.

How performance is monitored and reported

We monitor performance continuously through our support portal and platform monitoring tools. These track SLA compliance, system metrics, logs and audit trails in real time. We review results in structured service reviews, including quarterly business reviews, and agree clear actions for improvement. This approach ensures accountability and measurable progress.

3 G-Cloud alignment information

To help you unlock faster insights and measurable impact, we deliver every G-Cloud engagement through a structured yet adaptable model. This approach accelerates onboarding, ensures compliance and maintains clear governance at every stage. Our delivery philosophy reflects MDClone's mission: to democratise healthcare data safely and effectively. We combine ISO-aligned project controls with agile practices to reduce time to value while maintaining privacy, security and governance. Every phase is designed to empower your teams to use data confidently and at scale. We work with you through key phases:

Mobilise – Confirm scope, governance and infrastructure readiness to ensure a secure foundation.
Configure – Deploy the ADAMS platform, integrate agreed data sources and apply privacy-by-design security controls.
Enable – Train users, validate workflows and embed the Ask, Discover, Act, Measure, Share methodology for sustainable adoption.
Operate – Monitor performance, manage incidents and deliver continuous improvement through structured reviews and proactive support.
Exit – Support secure offboarding and data handover in line with your policies, ensuring full control remains with your organisation.

Aligned with Crown Commercial Service requirements, each phase is underpinned by clear roles, responsibilities and service levels. Our structured approach ensures transparency, accountability and measurable outcomes throughout the contract.

3.2 Onboarding and offboarding processes

This section explains how the service starts, operates and concludes under G-Cloud 15. The platform is deployed in your private infrastructure. You retain full control of systems and data. Data residency, backup and recovery follow your policies. There are no hidden costs or vendor lock-in. We agree any additional services in advance and exit activities fully align with Crown Commercial Service requirements.

3.2.1 Onboarding

To accelerate time to value and reduce complexity, we follow a clear, collaborative onboarding process. This ensures governance alignment and operational readiness from day one.

What happens once the contract is signed?

Process	Steps involved
Kick-off and scoping	We meet your governance and project teams to confirm objectives, scope, timelines and success criteria.
Statement of Work agreement	We finalise the Statement of Work (SOW), detailing scope, deliverables, dependencies and commercial terms.
Access and environment setup	You provide required system access, accounts and permissions. To maintain privacy and security, all work runs in your environment.
Resource allocation and scheduling	For transparency, we assign roles, confirm timelines and record milestones in the project plan.
Discovery and requirements confirmation	To validate functional, technical and user requirements, we run workshops. These form the baseline for delivery.
Security and governance alignment	In line with your policies, we configure identity controls, role-based permissions and communication structures. Using privacy-by-design principles, we deploy the ADAMS platform and integrate agreed data sources.
Training and readiness	We train administrators and end users through the MDClone Academy and validate operational readiness. Onboarding concludes when all stakeholders approve the SOW and project initiation documents.

3.2.2 Offboarding

To ensure a smooth exit and protect continuity, we use a structured offboarding process under buyer control. This confirms ownership of all assets and prevents vendor lock-in.

How we support secure exit

- **Project closure review**
  We confirm deliverables, capture lessons learned and assess performance against success criteria.
- **Documentation and handover**
  We provide configuration records, test outcomes, migration reports and training materials for your teams.
- **Knowledge transfer**
  So your teams operate confidently, our specialists deliver targeted workshops or shadowing sessions.
- **Access revocation and data return**
  You revoke any access granted to MDClone. Any temporary project data is returned or deleted under your policy.

- **Post-engagement support**
  Where required, we provide optimisation or advisory support through a new or extended SOW.

3.3 Data

3.3.1 Data importing and exporting

Data importing and exporting

To keep you in control, the platform runs inside your private infrastructure. Throughout the contract, you manage data flows, storage and export locations.

Data importing

- We ingest data from agreed source systems using a dedicated extraction server
- Extract, transform and load (ETL) activities run inside your environment for security
- We align connectivity with your network controls and policies
- Site to site virtual private network (VPN) is used where required
- Supported sources and formats are confirmed during onboarding. Examples include Databases like SQL Server, SAP HANA, Oracle, Databricks, etc.
- Unstructured clinical text is enabled through natural language processing (NLP) where deployed

Data exporting during the contract

- You control exports to approved locations using standard network protocols
- The platform supports on demand and scheduled export of approved outputs
- Export destinations are configured to your environment and governance model
- Export formats are agreed with you and may include CSV
- Synthetic data is available, where enabled, to support safe collaboration without exposing personal or identifiable data

End of contract data extraction

- At contract end, you receive a complete extraction in your chosen open format
- We include agreed records, audit trails and configuration artefacts
- Under your governance, we perform the handover inside your environment
- Storage and processing remain under your control as we do not hold your data
- We confirm access revocation and provide an exit summary for audit

Open formats and portability

- We design exports to use open, non-proprietary formats to support portability
- Typical open formats are agreed at call off. Examples include comma separated values (CSV)
- We avoid vendor lock in by keeping data structures documented and reusable
- Application specific elements are mapped to open representations where feasible

Controls and assurance

- All data flows operate within an isolated network segment, often called a demilitarised zone (DMZ)
- Data is encrypted in transit using transport layer security (TLS)
- Identity, role-based access and permissions align with your policies
- We record exports and changes in your monitoring and audit tools
- Penetration tests follow your schedule, with at least annual cadence

3.3.2 Analytics

To support decisions and governance, the platform includes built-in analytics and monitoring. You can view usage and performance in real time and act quickly.

What we provide

- Real-time dashboards that show system metrics, logs and detailed audit trails
- Configurable reports covering incidents, changes, and SLA performance
- Structured service reviews, including quarterly business reviews, with agreed actions

Service usage metrics

- We provide operational metrics to track adoption and performance. These can be tailored to your priorities
- Ticket volumes, by priority and status
- Response and resolution times against service level agreements (SLAs)
- Change success rate and maintenance notifications
- System health indicators, including resource utilisation and error events
- Audit trails for user actions and administrative changes

How metrics are delivered

Reports: Receive scheduled or on-demand reports for service reviews and audit.

Support for decision-making and governance

To strengthen governance, we align analytics to your policies and priorities. We document findings and actions in service reviews. We provide root cause analysis and post-incident reports for major events.

Business intelligence integration

We enable export to external business intelligence (BI) platforms through agreed formats. Typical formats will be confirmed at call-off. Examples include comma separated values (CSV)

Security of analytics data

Analytics operate within your isolated network segment. Data in transit uses transport layer security (TLS). Audit trails and logs are captured in your monitoring tools.

3.3.3 Independence of resource

To protect performance, each buyer runs the platform inside their own private infrastructure. No other customer shares your computer, storage or network resources.

How isolation is achieved

- The deployment is isolated in your dedicated network segment
- All storage and processing occurs within your environment under your governance
- MDClone accesses your environment only through a secure administration server using named accounts
- Unless you explicitly enable approved exports, data does not leave your organisation

Impact of other customers

As deployments are buyer-hosted and isolated, other customers cannot affect your performance.
There is no shared multi-tenant compute layer across buyers.

Capacity and load management

You control capacity using your native infrastructure, backup and replication tools. To reduce recovery time where implemented, the platform supports high availability configurations. To enable safe rollback, before major upgrades, we require a full system backup. We provide you with advanced notice of any planned maintenance, which we schedule outside business hours where possible.

Governance and assurance

To prevent cross tenant access, we align identity and role-based permissions to your policies. To evidence isolation and performance, monitoring captures system metrics, logs and audit trails. Following best practice, penetration testing occurs at least annually and after significant changes.

3.3.4 Public sector networks

To support secure operations, we align connectivity with approved public sector networks where required.

Network connectivity options

- By default, we do not expose the platform to public networks
- Connectivity to a public sector network is enabled only on request
- We confirm requirements during onboarding and document the controls

Governance and assurance

- Any connection follows the relevant accreditation and security standards
- Traffic is restricted to agreed endpoints and purposes
- Monitoring captures connection status, logs and audit trails
- We review configurations in service reviews to maintain compliance

3.3.5 Data-in-transit protection

To protect confidentiality and integrity, we encrypt all data in transit across the solution.

Between your network and the platform

- Transport layer security (TLS) version 1.2 or higher protects data in transit
- Site-to-site virtual private network (VPN) can be used where required
- Internet Protocol security (IPsec) is available for enhanced protection
- We restrict traffic to approved routes and ports under your policies

Within the platform

- Internal communication between components is encrypted using TLS
- Secure gateways enforce authentication and authorisation for application programming interfaces (APIs)
- Identity, role-based access and permissions align with your governance
- Logs and audit trails record access and changes for transparency

Protocols and restrictions

Legacy non-secure protocols are not supported.

3.3.6 Asset protection

To ensure data security and compliance, all storage and processing occur within your organisation's private infrastructure, either on-premises or in a private cloud region. This approach guarantees full control over residency and governance.

Data at rest is encrypted using Advanced Encryption Standard (AES-256) and remains isolated within your secure perimeter. We apply strict role-based access controls and enforce enterprise authentication methods such as Single Sign-On (SSO) and Security Assertion Markup Language (SAML). Our platform operates inside a dedicated demilitarised zone (DMZ) with network isolation through private endpoints and security groups. All traffic is encrypted in transit using Transport Layer Security (TLS) protocols.

Data sanitisation follows a multi-layered process. Source data is processed within the customer environment and anonymised during extraction, validated for quality and transformed into synthetic datasets that preserve statistical properties without containing personal data.. This enables safe collaboration while maintaining compliance with privacy regulations. End-of-life equipment disposal is managed according to recognised standards for secure destruction. Customers retain full ownership of all data assets and control retention periods. To align with your internal policies, we provide procedural guidance for backup, restore and disaster recovery.

As the platform is fully hosted within your infrastructure, users cannot specify external storage locations. No external sub-processors are used. Meeting your requirements, all compliance measures align with ISO 27001 and Cyber Essentials certifications.

3.4 Availability and resilience

3.4.1 Guaranteed availability

To protect continuity, we deploy the platform inside your private environment with network isolation in a dedicated demilitarised zone (DMZ). This design reduces external dependency and keeps control of resilience within your estate. To support proactive operations, a central monitoring cluster captures system health, logs and detailed audit trails. To enforce controlled access paths for support, we encrypt data in transit using Transport Layer Security (TLS).

How reliable the service is

To minimise service disruption during component failure, high availability (HA) configurations are supported. Backup and recovery align with your established enterprise policies, including storage replication where configured. To ensure a safe rollback path, before major upgrades, we require a full system backup.

Our resolution time depends on the priority as outlined earlier in this document.

What happens if there is a problem

You can raise incidents through the customer support portal with 24/7 ticket submission. Working hours for responses are business days, 08:00 to 17:00 local time. We triage, escalate to senior engineering when needed and provide root cause reviews for major incidents. For Priority 1 blocking issues, our service level agreement (SLA) targets a workaround or resolution within 48 working hours. We coordinate real time support through scheduled calls where critical issues require it.

How quickly things get back to normal

Recovery point objective (RPO) and recovery time objective (RTO) are defined by your infrastructure capabilities and policies. Our platform inherits your resilience controls, including snapshots and replication technologies. We support HA for automated failover to reduce recovery time where deployed. We validate restore procedures during upgrades by enforcing pre-upgrade backups.

We prevent incidents by isolating the platform in your DMZ, enforcing least privilege and monitoring all activity. We restore service using your enterprise backup regime, supported by our recovery guidance and HA options. We demonstrate a track record through defined SLAs, structured escalation and post-incident reviews.

3.5 Governance

To give you confidence, we run the service under proven, audited governance. We hold ISO/IEC 27001:2022 for information security management. We hold ISO 27799:2016 for health sector information security. We comply with Cyber Essentials requirements for Lot 2B to align with UK government expectations and our certificate number is 5341cc2e-df40-4f2f-b500-c25cb3457564

We also hold ISO27001:2022, related to big data technology for healthcare IT management. Our certificate number is 1123966.

We recognise Digital Technology Assessment Criteria (DTAC) as relevant for healthcare assurance and will complete this as required for each customer.

To drive consistency, we align our service practices with Information Technology Infrastructure Library (ITIL) version 4 principles. These practices support reliable delivery, safe change and continual improvement.

We review performance data, customer feedback and audit findings every month. These reviews identify improvement opportunities and track corrective actions to closure.

Our Compliance Manager oversees all management systems and governance activities. The Compliance Manager reports to the board level Quality and Security Committee to ensure accountability.

3.6 Security

To protect patient data, we embed security in every layer:

Security by design

Our platform is engineered with a security-first architecture that embeds protection and control into every layer of the environment:

- We deploy the platform inside your demilitarised zone (DMZ) with private endpoints and network security groups
- We enforce encryption in transit using Transport Layer Security (TLS)
- We enforce encryption at rest using Advanced Encryption Standard (AES-256)
- We control support access through a secure jump box with named accounts
- We maintain detailed audit trails to track all administrative actions

Policies controlled and enforced

Our operational framework is built on robust governance principles that ensure security, consistency and compliance across all environments and we:

- Align our practices to Information Technology Infrastructure Library (ITIL) version 4
- Apply least-privilege access and role-based access control for all users
- Require full system backups before major upgrades to enable rollback
- Operate change control and release management aligned to customer policies
- Prohibit uncontrolled data egress from the private environment

Standards and assurance

Ensuring our security and governance practices meet recognised industry and sector-specific benchmarks, we operate to rigorously validated standards and we hold:

- ISO/IEC 27001:2022 for information security management
- ISO 27799:2016 for health sector information security
- Cyber Essentials certificate for Lot 2B

As well as the above, we recognise Digital Technology Assessment Criteria (DTAC).

Oversight and governance

Our Compliance Manager oversees security governance and management systems. To ensure strong governance, the Compliance Manager reports to a board-level Quality and Security Committee.

The person responsible at board level is Luz Erez, CTO.

We review performance data, customer feedback and audits each month. We track corrective actions to closure and report trends to leadership.

Software Security Code of Practice

- We follow secure-by-design and privacy-by-design engineering practices
- We follow secure-by-design and privacy-by-design engineering practices
- We enforce code review, vulnerability management and configuration hardening
- We conduct penetration testing at least annually and after significant changes

Information security policies

We maintain documented policies covering access control, incident response and encryption.
We align platform operations to customer governance and residency requirements. To support data residency needs, we keep compute and storage in the same region. Reassuring you of our secure systems, we do not use external sub-processors for data storage or processing.

Incident management

You can raise incidents through the customer support portal at any time. We respond during business hours, 09:00 to 17:00 local time. For Priority 1 blocking issues, we target a workaround or resolution within 48 working hours. We provide root cause reviews for major incidents and agree preventive actions.

3.6.1 Operational security

Operational security ensures uninterrupted service and protects sensitive health data.

Configuration and change management

To minimise downtime, maintenance is scheduled outside business hours. To prevent disruption, all changes follow a documented process with clear approvals. Audit trails provide full visibility of configuration updates. Major upgrades include system backups to enable rollback if needed. Role based access control (RBAC) enforces least privilege during change activities. To detect early drift, we monitor configuration baselines. To drive continuous improvement, we facilitate post change reviews.

Vulnerability management

Following industry best practice, to reduce risk, vulnerabilities are patched quickly. To validate security, penetration testing occurs annually and after major releases. Encryption protects data in transit using Transport Layer Security (TLS) and at rest under agreed standards. Network isolation is achieved through private endpoints and network security groups (NSGs). Named accounts with full auditability govern support access. Security advisories are shared promptly after validation.

Protective monitoring

To detect threats early, monitoring runs continuously across all environments. For rapid analysis, logs, metrics and alerts are centralised. Critical events trigger real time notifications for immediate response. To maintain accountability, audit trails track privileged actions. Monitoring rules align with your risk profile and regulatory obligations. To refine controls, effectiveness reviews follow major incidents.

Incident management

To restore service quickly, Priority 1 issues receive a response within 4 working hours. Blocking errors have a resolution or workaround target of 48 working hours. For transparency, root cause analysis and post incident reports are shared. Communication follows agreed channels and timelines. To ensure long-term effectiveness, fixes are validated and monitored for recurrence.

Post-quantum cryptography compliance

To future-proof security, we plan for quantum resilience. Cryptographic dependencies are assessed and inventoried. Migration paths to post quantum cryptography (PQC) standards are defined. Hybrid approaches combining classical and PQC algorithms will support transition.

Compliance and assurance

Cyber Essentials certification is supported, and our information security practices align with ISO 27001 principles. Privacy by design and secure by design guide all delivery. Data residency and processing stay within your controlled environment. Synthetic data enables safe collaboration without exposing identifiable information.

Shared responsibility

Security responsibilities are clearly defined within a shared responsibility model. Roles and handoffs are documented in the order form. Controls are reviewed during onboarding and after any material change.

Customer responsibilities

Infrastructure-level controls remain under your management. Backup and recovery follow your internal policies. User onboarding and first-line data loading support are your responsibility. Approvals for changes affecting clinical operations must be provided promptly.

Evidence and reporting

Audit logs and change records are available on request. Penetration testing summaries and remediation progress are shared. Incident reports include lessons learned and action tracking. Quarterly reviews provide clear security metrics and trends.

3.6.2 Staff security

Strong staff security protects systems and patient data.

Vetting and authorisation

To reduce insider risk, access is limited to named personnel. Individual accounts are required for all support work. Least privilege is applied through role-based access control. Access is reviewed after role changes and during major releases.

Screening levels

Please note that this is not relevant to the service we provide.

Government security clearance

To support secure operations, government clearance can be arranged up to developed vetting (DV).

3.6.3 Secure development

Secure development reduces defects and speeds safe delivery.

Best practice

To prevent vulnerabilities, delivery follows secure-by-design and privacy-by-design principles. Security requirements are set early and tested throughout each stage. Code changes receive peer review and approval before release. Automated checks identify known issues and insecure dependencies. Threat modelling defines controls for high-risk components. Penetration testing occurs annually and after major and high-risk releases. Secure configuration baselines are maintained across all environments.

Independent review

To increase assurance, independent testing validates security controls as part our audited governance. We hold ISO/IEC 27001:2022 for information security management. We hold ISO 27799:2016 for health sector information security. We also comply with Cyber Essentials requirements.

3.6.4 Identity and authentication

Ensuring only authorised users gain access, there are strong identity controls in place.

User authentication

To simplify access and reduce risk, single sign-on is supported. Authentication works with SAML providers. Multi-factor authentication is recommended for all privileged roles.

Management access authentication

To protect admin paths, access uses named administrator accounts. A secure jump box controls support access in your environment. All administrator actions are logged with detailed audit trails. Session timeouts and just-in-time elevation reduce standing privilege.

Access restrictions in management interfaces

To prevent misuse, RBAC enforces least privilege for all roles. Administrative interfaces are isolated in a DMZ. Network access uses private endpoints and network security groups. Public traffic is blocked, and site-to-site VPNs provide secure connectivity.

3.7 Auditing

Auditing provides clear accountability and supports safe operations.

User activity audit

To strengthen governance, all user actions are recorded in detailed audit logs. Audit trails capture logins, data access, configuration changes, and exports. Logs include time stamps, user identifiers, and action context. Access to user activity logs is granted under agreed governance controls. Administrators can search, filter, and export audit records on demand.

Supplier activity audit

To ensure transparency, supplier support actions use named accounts. All supplier sessions pass through a secure jump box administration server. Administrator actions are logged in the central monitoring cluster. Customers can request supplier audit reports for defined periods.

Log retention

To align with your policy, logs are retained per local governance requirements. Retention periods follow your organisational standards and clinical needs. System logs remain available for investigations and compliance audits.

MDClone does not keep any user logs. Any recorded logs are only for the customer. Our platform enables the System Administrator to view logs and usage, however, this is in the hands of the buyer.

Access to audit information

To speed investigations, authorised users access audits through the platform interface. Role based access control RBAC limits who can view or export audit data. Secure access can be integrated with single sign on SSO using SAML. Customers can receive regular audit extracts via agreed secure methods.

Assurance

To improve trust, audit scope and retention are confirmed during onboarding. Controls are reviewed after major releases and material changes. Post incident reviews include audit analysis and lessons learned. Our Chief Technology Officer is the individual responsible for audit queries and escalation.

3.7.1 Performance monitoring and metrics

We provide continuous monitoring to give you full visibility and confidence in service performance. A central monitoring cluster tracks system health, logs, and audit trails in real time. You will receive clear usage and performance metrics through dashboards and scheduled reports. These include adoption measures based on our volume and value framework within the ADAMS Center methodology.

We track priority 1 incidents against our service level agreement, aiming for resolution or workaround within 48 working hours. Post-incident reviews and root cause analysis ensure issues do not recur.

Shared success metrics are reviewed with you during quarterly service and business reviews. You can monitor ticket status and progress through our customer support portal.
For transparency, reporting aligns with FinOps Open Cost and Usage Specification (FOCUS) standards. We agree reporting cadence, recipients and thresholds with you during onboarding.

3.7.2 Compliance and quality management

To protect patient data and maintain trust, we operate with rigorous security and quality controls. Our approach is based on secure-by-design and privacy-by-design principles.

We hold ISO/IEC 27001:2022 for information security and ISO 27799:2016 for health data security. Cyber Essentials certification is maintained for Lot 2B and provided at call-off.

Penetration testing is performed annually and after major changes. Data is encrypted at rest and in transit using TLS. Supporting residency requirements, all processing occurs within your private infrastructure. For accountability, we maintain detailed audit trails and centralised logging. Access is controlled through named accounts via a secure administration server. Single sign-on (SSO) using Security Assertion Markup Language (SAML) is supported where required.

To minimise downtime, change management follows scheduled maintenance windows with advance notifications. Delivery aligns with Agile practices and healthcare governance standards.
Reporting also follows FOCUS standards for cost and usage transparency. We do not use external sub-processors and any large language model (LLM) runs inside your secure subnet when enabled.

3.8 Backup, restore and disaster recovery

To protect continuity and trust, we design backup and recovery around your environment. The platform is customer-hosted within your secure perimeter.

Overview and governance

To identify risks and define recovery procedures, we operate a Business Continuity Management (BCM) framework. A named recovery lead activates protocols, coordinates communications and oversees restoration. To verify readiness, we review risks twice a year and run annual disaster recovery exercises. All activities align with your governance, security policies and operational priorities.

Backup and data protection

Backups follow your organisation's policies and technical standards. We work with your IT team to align schedules, retention and media handling. MDClone requires a full system backup before any major platform upgrade. Data at rest is encrypted using industry standard controls. Data in transit is encrypted using Transport Layer Security (TLS). Storage and replication use your native technologies and controls.

Disaster recovery and restoration

Our Disaster Recovery Plan (DRP) sets recovery priorities and escalation paths. Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are defined by your organisation. The platform supports high availability (HA) configurations to minimise downtime. We maintain VPN-controlled access for support, using named accounts and full audit trails. We schedule maintenance outside business hours where possible, with advance notifications.

Operating model and safeguards

The platform runs inside your demilitarised zone (DMZ) on private infrastructure. Compute and storage remain in the same region to meet residency requirements. Single sign on (SSO) using Security Assertion Markup Language (SAML) is supported. Centralised logging and audit trails provide full accountability for all actions. We do not use external sub-processors for data storage or processing. Any large language model (LLM) runs inside your secure subnet when enabled.

Business continuity measures

We follow your backup and replication controls, including local or zonal resilience. Cloud deployments can align to locally redundant storage (LRS) or zone redundant storage (ZRS). A tiered support model provides rapid triage and escalation for priority incidents. For a priority 1 blocking error, we target a workaround or resolution within 48 working hours. To ensure reliable rollback if needed, we require a pre-upgrade backup.

Continuous improvement and assurance

We conduct post-incident reviews and integrate lessons learned into procedures. We share success metrics during quarterly reviews to evidence service resilience. Reporting can align to FinOps Open Cost and Usage Specification (FOCUS) where applicable.

3.9 Training

To accelerate adoption and empower your teams, we provide structured training designed for different roles and learning styles. Our approach combines self-paced resources, live sessions and practical enablement.

Training formats

Our diverse training formats are outlined below.

Online self-paced learning: Access the MDClone Online Academy for interactive modules, video tutorials, and role-based learning tracks.
Instructor-led sessions: Live or hybrid courses tailored to your organisation's needs, including onboarding and advanced workflows.
Train-the-trainer programmes: Enable internal champions to scale knowledge across teams.
Webinars and masterclasses: Cover new features, best practices, and real-world use cases.
Podcasts and on-demand content: Share thought leadership and success stories to inspire innovation.

Learning artefacts

To support ongoing learning, we provide comprehensive resources, including:

- Step-by-step guides and handbooks
- Over 100 short "how-to" videos embedded in the platform
- Recorded webinars and masterclasses available on demand
- Digital certificates to recognise learner progress

Accessibility and delivery

For scalable access and progress tracking, training is delivered through the MDClone Online Academy, built on a learning management system (LMS). All content is designed for clarity and ease of use.

Pricing

Access to the Online Academy, including e-learning, tutorials, and recorded webinars, is included in the standard license. Instructor-led training and customised workshops are available as chargeable services, scoped and priced separately.

Continuous improvement

To reflect new features and best practices, we collect feedback after each session and update content regularly. This ensures your teams stay informed and confident in using the platform.

3.10 Service pricing

Our pricing approach is designed to provide the best possible value for money combined with flexibility on a tailored deployment to suit all customers and can work up bespoke options to suit local information governance, infrastructure requirements and processes.

Our goal is to enable health systems to deliver data-driven improvement in patient care, continuous performance improvement, faster research and safer collaboration. MDClone's ADAMS platform enables health systems across the world to do exactly this and our pricing approach reflects the self service capabilities withing our platform – we provide a platform where health systems are not reliant on scarce internal/external analytical resources and our set up and training enables organisations to be self sufficient in key tasks such loading additional data or enriching your data through our self service NLP suite yourselves meaning you are not locked in to needing additional services from us.

For health systems that do choose additional support we have a team of experts to suit your needs
Our commercial approach always includes:

- A one off set up fee which includes onboarding
- A license agreement

If needed, we can provide the following additional services:

- Data Load
- Use Case cohort creating
- Training
- NLP Development

We have significant experience of deploying across a range of Electronic Patient Record systems including in- house solutions.

3.11 Invoicing process

To streamline billing and cash flow, we align to standard government terms. Invoices for services are issued on agreed milestones after delivery. The annual license is invoiced once per year in line with contract dates. Payment terms are 30 days from invoice date under government policy.

Accepted payment methods include **BACS and PO**. We do not provide a self-billing portal for invoice submission. The minimum contract term is two years (or 1 year, subject to discussion). If required, we can supply a billing schedule template during onboarding.

3.12 Termination terms

Termination is governed by the Crown Commercial Service G-Cloud 15 Call-Off Terms and Conditions. Buyers may terminate the contract in accordance with these terms by providing written notice. MD Clone may terminate only in cases of material breach or non-payment. To maintain transparency and control, we define clear steps for contract termination.

End of contract term

When the contract reaches its natural end, all rights and licenses granted under the agreement will terminate. You retain full ownership of all data assets created during the engagement. We deactivate access to MDClone support services and mark the account as inactive in our systems.

Early termination

Either party may terminate the agreement if a material breach occurs and is not resolved within 30 days of written notice. Immediate termination applies if either party enters insolvency proceedings or similar arrangements. Upon termination, you must stop using the platform and return or securely destroy all copies of the software. We require written confirmation that all copies have been removed or destroyed.

Surviving obligations

Confidentiality, intellectual property rights, and liability clauses remain in effect after termination. Sections covering usage restrictions, ownership, and confidentiality continue to apply.

Data handling

All data remains within your infrastructure throughout the engagement. Data retention and deletion follow your organisation’s policies. We provide guidance for secure removal of platform components if requested.

4 Security and data governance

To protect patient data, we design security around your environment. The platform is customer-hosted inside your secure perimeter. We apply secure by design and privacy by design principles across delivery. We maintain clear governance, auditable operations, and controlled access.

We hold ISO/IEC 27001:2022 for information security and ISO 27799:2016 for health data security. Cyber Essentials certification applies to Lot 2B engagements. We perform penetration testing at least annually and after significant changes. We maintain centralised logging and full audit trails for accountability. Access is through named accounts via a secure administration server. We support single sign on (SSO) using Security Assertion Markup Language (SAML). We do not use external sub processors for data storage or processing. Any large language model (LLM) runs inside your secure subnet when enabled.

4.1 Data protection and encryption

To protect data in transit, we use Transport Layer Security (TLS) version 1.2 or higher. Site to site virtual private networks (VPNs) secure connectivity where required. We enforce encryption at rest using industry standard controls. Key management follows customer policies and approved procedures. We isolate traffic using firewalls and network security groups. Private endpoints and network segmentation prevent exposure to the public internet.

We protect data between networks using private connectivity and VPN gateways. We restrict access to named support accounts with full logging. We protect data within the network using a demilitarised zone (DMZ). Compute and storage remain inside your private infrastructure. We monitor events using a central monitoring cluster. Logs and audit trails are captured for all administrative actions.

4.2 Data at rest, storage locations, and physical security

Data is stored and processed entirely within your infrastructure. You control the storage technologies, regions, and resilience settings. Compute and storage stay in the same geographic region to meet residency requirements. Storage and replication use your native tools. We support locally redundant storage (LRS) and zone redundant storage (ZRS) where applicable. High availability (HA) configurations help minimise downtime. Physical security is managed by your hosting facilities. Controls follow your standards for access, surveillance, and incident response. We encrypt data at rest using customer approved methods. Access to datasets is governed by role-based policies and named accounts.

4.3 Data sanitisation and disposal

We apply privacy by design to protect sensitive information. Our approach uses several complementary safeguards within your environment. Extraction and anonymisation occur on the extract transform load (ETL) server. This process moves data into the platform’s big data cluster. The synthetic data engine

generates privacy preserving datasets. These mirror statistical properties but contain no real personal information.

The Cross Platform Assurance (CPA) module validates data quality during loading. Guardrails inspect prompts and segmented data for AI features. Access is authorisation based, with policies at user and feature level. Users only see data they are explicitly allowed to view. Secure deletion follows your policies and approved methods.

MDClone follows buyer approved standards and does not impose a fixed sanitisation method.
MDClone does not mandate specific disposal vendors and does not engage third party disposal partners without explicit buyer request and approval.

4.4 Security testing and assurance

To maintain trust and resilience, we test our platform regularly for vulnerabilities. Penetration testing is performed at least annually and after major system changes. Testing follows recognised standards and is conducted by qualified professionals. We use structured methodologies aligned with industry best practice.

We run automated vulnerability scans on core components. Findings are prioritised by severity and remediated within agreed timelines. Fixes are tested before deployment to prevent disruption. Data sanitisation is part of our privacy-by-design approach. We apply cryptographic erase or secure wipe methods based on buyer standards. Certificates of deletion are available on request. Hardware disposal follows recognised standards or approved third-party processes. Data bearing assets are sanitised using NCSC-approved methods.

4.5 Incident and protective monitoring management

To protect your environment, we monitor and respond to security events proactively. Incidents are triaged through our customer support portal and escalated by severity. Priority 1 issues receive immediate attention and targeted resolution efforts. We classify incidents and follow ISO 27035 principles for response and reporting.
We maintain detailed audit trails for all administrative actions. Post-incident reviews identify root causes and feed continuous improvement. Vulnerability management is integrated into our processes. We track issues, apply fixes, and verify remediation before closing tickets in alignment with the response times outlined earlier in this document.

4.6 Configuration and change management

To ensure stability and security, we apply controlled, auditable change processes. Our approach aligns with Information Technology Infrastructure Library (ITIL) principles for change management. We assess all changes for security impact before implementation.

To minimise risk, version control and rollback procedures are in place. Where possible, major changes are scheduled outside business hours. To reduce operational disruption, advance notifications are provided. Access control supports governance and accountability. We enforce role-based permissions and limit administrative access to named accounts. Authentication supports enterprise single sign-on (SSO) using Security Assertion Markup Language (SAML). Remote support uses a secure jump box with VPN-controlled access.

4.7 Information security management and certifications

We operate under a robust governance framework validated by third-party standards. Our processes align with ISO/IEC 27001:2022 for information security and ISO 27799:2016 for health data security. Cyber Essentials certification applies to Lot 2B engagements.

Annual audits and surveillance reviews verify compliance and strengthen assurance. For business continuity and disaster recovery, we maintain documented policies. Backups follow your organisation's policies and are required before major upgrades. To oversee governance, we appoint a named Information Security Manager.

4.8 Secure development and cryptography

To protect your data and maintain system integrity, we apply secure development practices throughout the software lifecycle. We follow a Secure Software Development Life Cycle (SDLC) that includes:

- Code reviews for every release
- Automated dependency scanning to identify vulnerabilities early
- Static and dynamic analysis tools to validate security posture

Our development process complies with the Open Web Application Security Project (OWASP) Top 10 guidelines to prevent common application risks. We apply cryptographic controls based on industry standards, including:

- Data in transit is encrypted using Transport Layer Security (TLS) version 1.2 or higher
- Data at rest is encrypted using Advanced Encryption Standard (AES) 256-bit encryption
- Key management follows strict governance and customer-approved policies

To future-proof encryption strategies, we monitor emerging threats and align with National Cyber Security Centre (NCSC) guidance on post-quantum cryptography.

4.9 Identity and access management

To safeguard access and maintain accountability, we enforce strong identity and access controls. Our approach includes:

- **Multi-factor authentication (MFA)** for all administrative accounts
- **Role-based access control (RBAC)** to ensure users only access what they need
- **Configurable permissions** aligned with organisational governance

We support enterprise authentication standards, including:

- **Single Sign-On (SSO)** using Security Assertion Markup Language (SAML)
- **OAuth 2.0** integration for secure delegated access where required

Administrative access is limited to named accounts with full audit trails. To prevent unauthorised entry, remote support uses a secure jump box with VPN-controlled access.

5 Supplier information

5.1 About us

MDClone was founded in 2016 and operates globally from its headquarters in Beer-Sheva, Israel. We work with leading health systems, academic medical centres, life sciences organisations and public sector bodies across North America, Europe, and the UK.

Our mission is clear, democratise healthcare data to improve care, operations, and research. We remove technical and privacy barriers so clinicians, analysts and researchers can safely access and use data at scale.

Our core platform, MDClone ADAMS, enables self-service data exploration without coding. Allowing organisations to collaborate securely and accelerate insight generation, it combines advanced analytics with privacy-preserving synthetic data. This approach reduces time to answer from months to days and supports measurable improvements in quality, efficiency and outcomes.

We reinforce trust through secure-by-design and privacy-by-design principles. MDClone holds ISO/IEC 27001:2022 and ISO 27799:2016 certifications for information security and health sector data protection. We also align with Cyber Essentials requirements for UK public sector engagements.

Our values guide everything we do:

- **Privacy and trust by design** – protecting patient data and meeting governance standards
- **Empowerment of users** – enabling frontline teams to access and act on data
- **Impact-driven delivery** – focusing on measurable improvements, not technology for its own sake
- **Collaboration and openness** – supporting safe partnerships across organisations
- **Responsible innovation** – applying AI and analytics ethically and securely

We help you unlock the full value of your data while maintaining control, compliance, and confidence.

5.3 Relevant experience

Our experience demonstrates how Lot 2B services enable secure, governed access to healthcare data and support operational improvement.

Intermountain Healthcare

To improve kidney disease care, clinicians increased protocol adherence from 32% to 80% using governed self-service analytics. This was delivered through infrastructure software that enforced role-based access, audit trails, and secure configuration—core Lot 2B capabilities. To reduce utilisation, unplanned admissions fell by **50%**, supported by repeatable workflows embedded in the platform.

This initiative delivered an estimated **$12 million** in savings and contributed to Intermountain receiving a HIMSS Davies Award.

Washington University School of Medicine

To accelerate research, the platform enabled rapid cohort discovery through secure infrastructure software deployed behind the firewall. Aligning with Lot 2B requirements, identity and authentication controls ensured only authorised users accessed sensitive data. Synthetic data technology allowed early-stage exploration without exposing patient identifiers, reducing governance risk and supporting compliance.

Public sector innovation partnerships

To speed innovation, partners used synthetic data within a secure environment before validating real data under strict governance. This approach leveraged Lot 2B features, such as configuration management, audit logging and controlled access. Demonstrating the flexibility of our infrastructure software for high-impact use cases, priority areas included COVID-related work, suicide prevention and cardiovascular disease prevention.

Independent recognition

Reflecting our leadership in secure, scalable healthcare data solutions, MDClone was named a World Economic Forum Technology Pioneer in 2021. MedTech Breakthrough awarded MDClone Best Healthcare Big Data Platform for three consecutive years (2021–2023).

5.4 How to buy

MDClone services can be procured directly through the Crown Commercial Service (CCS) G-Cloud 15 Digital Marketplace. Buyers can search for MDClone on the Digital Marketplace and select the required service listing. Once selected, the buyer and MDClone will:

- Agree a Statement of Work (SOW) detailing scope, deliverables, timescales and pricing
- Raise a Call-Off Contract under the G-Cloud framework terms
- Issue a Purchase Order (PO) to confirm commencement
- Ensure transparency and compliance with public sector regulations in line with G-Cloud framework conditions

Enquiries or pre-contract discussions can be arranged through our central contact point:
Name: Matthew Whitty/Director of Commercial Partnerships
Email: sales@mdclone.com