



G-Cloud 15 (RM1557.15)

CLEO Systems 24 LTD

**CLEO Virtual Waiting Room (VWR)
Service Definition**

January 2026

Table of contents

1 Introduction	4
1.1 Document structure.....	4
1.2 How to use this document	4
2 Service description	5
2.1 About our service	5
2.2 Delivery framework.....	5
2.3 Service features / benefits	6
2.4 Service scope	8
2.4.1 Add-ons and extensions	8
2.4.2 Cloud deployment model	8
2.4.3 Service constraints	8
2.4.4 System requirements.....	9
2.5 User support.....	9
2.5.1 Support details.....	9
2.5.2 Accessibility and usability	10
2.6 How users work with our service.....	11
2.6.1 Browsers	11
2.6.2 Desktop application	11
2.6.3 Mobile.....	11
2.6.4 Service interface	11
2.6.5 API	11
2.6.6 Accessibility and usability	12
2.6.7 Customisation	12
2.6.8 Service levels and availability.....	12
3 G-Cloud alignment information	14
3.1 Section introduction	14
3.2 Onboarding and offboarding processes.....	14
3.2.1 Onboarding	14
3.2.2 Offboarding.....	14
3.3 Data	15
3.3.1 Data importing and exporting	15
3.3.2 Analytics	15
3.3.3 Independence of resource	16
3.3.4 Public sector networks	16
3.3.5 Data-in-transit protection	16
3.3.6 Asset protection	16
3.4 Availability and resilience	16
3.4.1 Guaranteed availability	16

3.5 Governance	17
3.6 Security	17
3.6.1 Operational security	18
3.6.2 Staff security	18
3.6.3 Secure development	18
3.6.4 Identity and authentication	18
3.7 Auditing	19
3.7.1 Performance monitoring and metrics	19
3.7.2 Compliance and quality management	19
3.8 Backup, restore and disaster recovery	20
3.9 Training	21
3.10 Service pricing	21
3.11 Invoicing process	22
3.12 Termination terms	22
4 Security and data governance	23
4.1 Data protection and encryption	23
4.2 Data at rest, storage locations and physical security	23
4.3 Data sanitisation and disposal	23
4.4 Security testing and assurance	23
4.5 Incident and protective monitoring management	23
4.6 Configuration and change management	24
4.7 Information security management and certifications	24
4.8 Secure development and cryptography	24
4.9 Identity and access management	24
5 Supplier information	25
5.1 About us	25
5.2 CLEO VWR development and rationale	25
5.3 How to buy	25

1 Introduction

1.1 Document structure

This Service Definition outlines how CLEO VWR will be delivered under the G-Cloud 15 framework. We have structured the document to give public-sector customers clear, accessible information about the service. This includes its functionality, delivery model, technical requirements, security standards and commercial terms. To support customers at different stages of the procurement lifecycle, we have organised this document into 5 main sections:

- **Section 1 – Introduction:** Provides an overview of the purpose of this document, how it is organised and how it should be used by customers evaluating CLEO VWR
- **Section 2 – Service description:** Describes what CLEO VWR is, the problems it solves, the service features and benefits, technical requirements, service levels and how end-users interact with the system
- **Section 3 – G-Cloud alignment information:** Demonstrates how CLEO VWR meets the specific requirements of the G-Cloud 15 framework, including onboarding/offboarding processes, data controls, service availability, governance, security and auditability
- **Section 4 – Security and data governance:** Details how CLEO VWR protects patient data, maintains compliance with NHS and UK Government standards and embeds security throughout its technical and operational environments
- **Section 5 – Supplier information:** Provides background on CLEO Systems, our experience, customer base and how to purchase CLEO VWR through the G-Cloud Digital Marketplace

We have structured each section to allow customers to quickly locate the information most relevant to their stage in the procurement process.

1.2 How to use this document

This Service Definition has been designed to guide customers through the G-Cloud procurement process and provide clear, structured information about CLEO VWR. It can be used to:

- Assess service suitability with Section 2 summarising what CLEO VWR does, the settings it supports and the problems it solves, helping alignment with NHS needs
- Complete technical and security due diligence as Sections 3 and 4 outline hosting, data protection, onboarding, availability, resilience, compliance and governance
- Plan implementation and operational readiness through Section 3's detailing of onboarding activities, prerequisites, roles and training expectations
- Support commercial and contractual review with Section 3.10-3.12, providing pricing models, invoicing approach and termination terms
- Verify supplier capability as we have outlined our organisation background, accreditations and relevant NHS experience in Section 5

2 Service description

2.1 About our service

CLEO VWR is a cloud-based, Software-as-a-Service (SaaS) solution designed to transform patient flow management in urgent and unscheduled care settings. Instead of relying on manual outbound calling and static queues, VWR intelligently automates the process of contacting patients and placing them into a virtual waiting room, ready for the next available clinician.

By dynamically managing call queues in real time, CLEO VWR reduces delays, eliminates missed contacts and improves resource use. Minimising waiting times and maximising throughput, our solution monitors clinician availability and consultation cadence, automatically adjusting when patients are contacted. This approach has increased our clients **number of consultations per hour by 50% on average** while improving patient experience and safety.

CLEO VWR is system-agnostic and can operate as a standalone service or integrate with CLEO Integrated Urgent Care products. Allowing customers to define queue logic, escalation rules and reporting requirements, we have designed CLEO VWR to be highly configurable to local priorities. Built to NHS standards, CLEO VWR complies with the DCB0129 clinical safety requirements and supports secure, resilient operation within UK-based private cloud infrastructure. The key outcomes delivered by CLEO VWR includes:

- Increased clinician productivity through automated queue management
- Enhanced patient satisfaction with real-time updates and reduced waiting times
- Elimination of “no shows” through Interactive Voice Response (IVR) confirmation
- Improved operational planning through data-rich reporting and analytics

2.2 Delivery framework

We deliver CLEO VWR through a structured, clinically informed implementation framework designed to ensure a smooth, safe and efficient transition to live service. To minimise disruption and accelerate adoptions, our approach combines technical readiness, operational alignment and robust governance. The key principles of our delivery framework include:

- **Collaborative planning:** We work closely with customer stakeholders to confirm scope, objectives and success criteria
- **Configuration and optimisation:** We configure CLEO VWR to reflect local priorities, including queue logic, escalation rules, clinician pools and reporting requirements
- **Clinical safety assurance:** All deployments comply with DCB0129 standards, supported by customer completion of DCB0160 prior to go-live
- **Structured onboarding:** We provide Train-the-Trainer sessions, user guides and User Acceptance Training (UAT) support to ensure readiness
- **Controlled go-live:** Our Project Team supports deployment remotely or on-site, followed by a 2-week hyper care period before transition to Business As Usual (BAU)
- **Continuous improvement:** Post-implementation reviews and account management meetings ensure ongoing optimisation and alignment with evolving needs

Our visual delivery framework and lifecycle diagram:

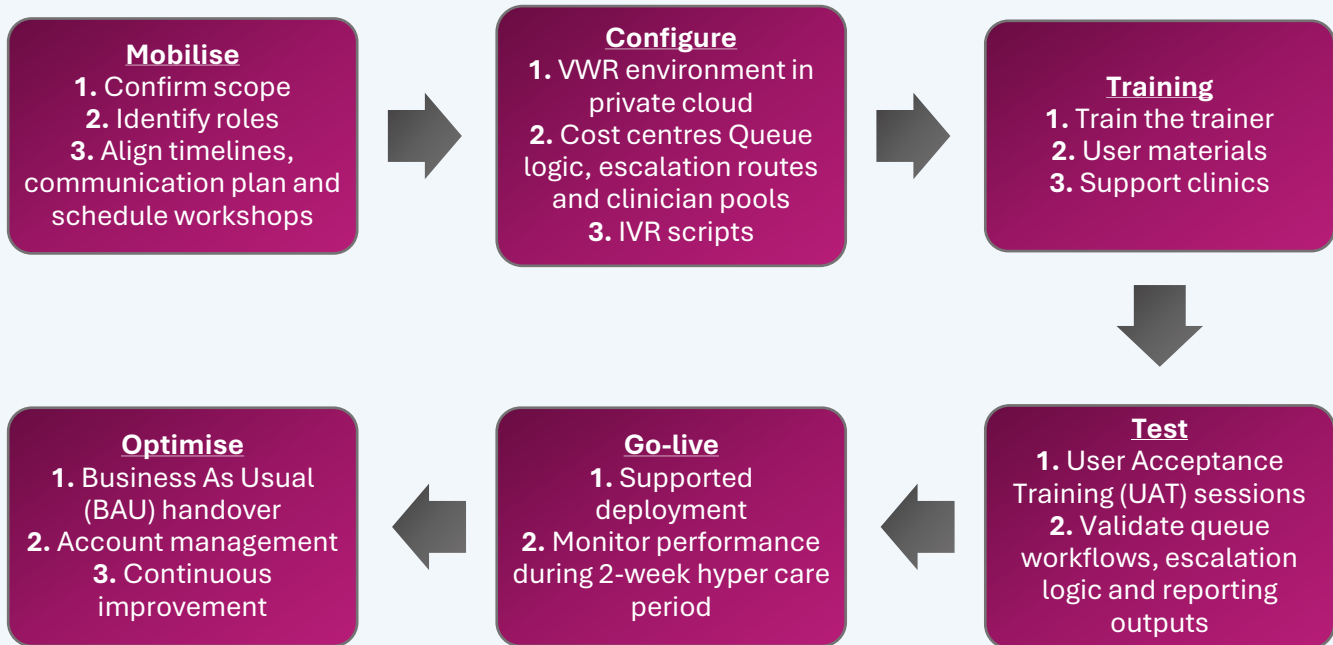


Figure 2.2.1: Our visual delivery lifecycle diagram

2.3 Service features / benefits

Our CLEO VWR service provides the following features:

- **Fully automated queue management:** Real-time automation of patient queues reducing delays, improving throughput and minimising manual intervention
- **Dynamic patient contact and IVR confirmation:** Automatically calls patients and confirms their availability before placing them in the virtual waiting room, eliminating no shows
- **Smart escalation and prioritisation:** Configurable rules ensure urgent cases are prioritised and workloads balanced across available clinicians
- **Real-time communication and status updates:** Keeps patients informed throughout the process, improving transparency and experience
- **Data-rich reporting and analytics:** Provides actionable insights into queue performance, clinician use and patient management
- **Compliance with DCB0129 clinical safety standards:** Ensures safe deployment and operation in line with NHS requirements
- **System-agnostic integration:** Works standalone or integrates with CLEO Integrated Urgent Care products and other compatible systems through OpenAPI interfaces
- **Configurable queue logic and business rules:** Allows customisation of workflows to meet local service priorities
- **Role-based access control:** Provides secure, permission-based access for clinicians and administrators
- **Real-time performance dashboards:** Displays queue status, clinician availability and patient engagement metrics at a glance

By providing these features, CLEO VWR provides a suite of key benefits for our customers, including:



Faster patient flow with automated queue management to reduce delays and shorten waiting times



Increased clinician productivity through the removal of manual calling tasks, enabling more consultations per hour



Reduced missed contacts with IVR confirmation ensuring patients are present, eliminating no shows



Improved patient experience with real-time updates giving patients confidence and transparency in their care journey



Smart clinical prioritisation, ensuring the most urgent cases are handled first



Better resource planning with data-rich reporting supporting forecasting and operational decision-making



Seamless workflows with conditional system integration enabling CLEO VWR to work standalone or with integration with CLEO Integrated Urgent Care



Enhanced governance and compliance as CLEO VWR has been built to NHS standards, including DCB0129 and the NHS Data Security and Protection Toolkit (NHS DSPT)



Scalable and resilient performance as CLEO VWR handles peak demands through its robust cloud architecture and disaster recovery procedures



Cost efficiency due to reduced administrative overhead and optimised clinician time for direct patient care

2.4 Service scope

CLEO VWR is a SaaS patient management solution delivered as a private-cloud service, designed to support NHS clinical teams. To optimise implementation and ensure compliance, we define the scope of CLEO VWR through 4 elements:

1. Service characteristics
2. Add-ons and extensions
3. Cloud deployment model
4. Operational constraints and system requirements

This structure helps customers understand how CLEO VWR fits into their environment and which conditions will support a smooth adoption.

2.4.1 Add-ons and extensions

CLEO VWR can be used standalone or can be integrated into other CLEO Integrated Urgent Care products.

2.4.2 Cloud deployment model

Providing controlled data residency, strong security and predictable performance in compliance with NHS DSPT, we deliver CLEO VWR as a private-cloud SaaS service through UK AWS regions only. To deliver this, we:

- Ensure data remains fully sovereign by hosting all components within UK-based private cloud infrastructure
- Protect performance and support safe patient management through use of a single-tenant-per-customer model
- Confirm performance during peak activity by designing all environments for scalability
- Enable consistent patching, maintenance and availability by managing the environment centrally

2.4.3 Service constraints

For the successful deployment and operation of CLEO VWR, the following constraints apply:

- Users must have NHS Smartcards with appropriate Roles and Activities configured
- Access to the Health and Social Care Network (HSCN) is required at all operational locations
- Oberthur middleware must be installed to support Smartcard authentication in line with NHS England requirements
- All environments must pass local UAT before go-live
- End-user devices must meet the minimum specifications for browser compatibility and audio/video functionality
- Maintenance will be scheduled by agreement with the customer to minimise disruption
- Changes to configuration or service scope require prior agreement with the customer
- CLEO VWR is not designed for use on mobile devices
- Service is intended for UK-based use only due to reliance on NHS infrastructure

2.4.4 System requirements

Requirement	Details
Operating System (OS)	Any OS capable of running modern browsers such as Windows, macOS or Linux
Supported browsers	Microsoft Edge (v142 or later), Google Chrome (v142 or later)
Screen resolution	Minimum 1024 x 768 pixels
Internet connection	Minimum 400 kbps for low-quality calls with 4 Mbps download and 1.5 Mbps upload speeds recommended
Audio/video hardware	Device with functional microphone and camera (for video consultations)
Installation	No client installation required as CLEO VWR is a cloud-hosted solution
Additional components	None required beyond browser, must ensure latest browser updates are applied
Network access	Reliable HSCN connectivity, with firewalls configured to allow service endpoints
Security requirements	NHS Smartcard access for authentication and Oberthur middleware where applicable

Figure 2.4.4.1: CLEO VWR system requirements

2.5 User support

To help users resolve issues quickly and maintain queue continuity and patient flow, we provide a structured, ITIL-aligned support service. To deliver this, our Service Desk triages requests, allocates skilled specialists and ensures rapid, consistent support across all clinical settings. Strengthening operational continuity, we combine multi-channel access, clear escalation routes and proactive account management.

2.5.1 Support details

How users contact us

User can access support through the following channels:

- **Customer Portal:** For logging incidents, service requests and change requests
- **Email:** For non-urgent queries
- **Telephone:** For Priority 1 (Critical) incidents, available 24/7

Ensuring all support is delivered by trained specialists, we do not provide web chat or AI-driven chatbots.

Support hours

To maintain continuity in clinical services, we provide the following support hours:

- **Core support hours:** 08:00-18:00, Monday-Friday (UK time)
- **Critical incident support:** 24/7 by telephone for Priority 1 cases
- **Portal access:** Available 24/7 for logging and tracking cases

Response times

- ✓ **PRIORITY 1:** 1 hour to respond, 4 hours to resolve
- ✓ **PRIORITY 2:** 2 hours to respond, 16 hours to resolve
- ✓ **PRIORITY 3:** 8 hours to respond, 5 business days to resolve
- ✓ **PRIORITY 4:** 8 hours to respond, 30 business days to resolve

Demonstrating our rapid response times, we maintain **99.9% service availability and use all reasonable endeavours to respond to and resolve 100% of support requests within their allocated time.**

Accessibility of support channels

To support all users, our Customer Portal is actively progressing toward WCAG 2.2 AA compliance, with all features supporting keyboard navigation and screen-reader access.

Named support roles

To strengthen governance and communication, we provide the following customer support roles within our Account Management Team:

- A **Customer Success Manager** who provides strategic engagement, reviews performance and aligns the service to buyer priorities
- A **Support Manager** who oversees operational responses and ensures timely incident progression
- A **Project Manager** who supports onboarding and all major service changes

Third-party access

To support shared-service models and multi-agency working, where authorised by the customer, third-party contractors can access the Customer Portal and raise cases.

Escalation routes

The escalation model below ensures rapid action when incidents impact clinical service:



Figure 2.5.1.1: Our escalation routes

This approach protects clinical operations and ensures transparent communication at every stage.

2.5.2 Accessibility and usability

We design our support and user-facing services to be accessible to all clinical and administrative users, including those who rely on assistive technologies. To support equitable access for every user group, we:

- Design all support services in alignment with WCAG 2.2 AA principles
- Ensure the Customer Portal is accessible through keyboard navigation and screen readers
- Provide documentation in PDF format designed for accessibility, with alternative formats available upon request
- Review accessibility feedback through our robust continuous improvement process

To maintain accessibility across new releases, we undergo comprehensive testing and assurance procedures. Prior to deployment, we assess major updates for accessibility. We review portal usability with real users and integrate emerging accessibility needs into development. Supporting inclusive digital access, we ensure that TOPdesk, our ITSM platform provider, actively develops toward full WCAG 2.2 AA compliance. This includes including compliance as a minimum quality requirement, expert oversight from the TOPdesk team and automated and manual testing such as screen reader testing.

2.6 How users work with our service

2.6.1 Browsers

CLEO VWR operates in any up-to-date web browser such as Microsoft Edge and Google Chrome (v142 or later).

2.6.2 Desktop application

CLEO VWR does not require a desktop application for operation. The service is fully cloud-hosted and accessed through modern web browsers.

2.6.3 Mobile

CLEO VWR is not designed for use on mobile devices.

2.6.4 Service interface

To support efficient clinical use, CLEO VWR provides a simple, intuitive web-based interface designed for ease of use and operational efficiency. This interface can be accessed through a modern browser and requires no desktop installation. Our interface features include:

- **Queue dashboard:** Displays real-time patient queue status, clinician availability and call progress
- **Clinician view:** Enables clinicians to take the next available call from the shared queue with a single click
- **Patient status indicators:** Shows confirmation of patient availability through IVR and estimated wait times
- **Configurable prioritisation:** Allows authorised users to adjust queue logic and escalation rules based on clinical need
- **Reporting panel:** Provides access to performance metrics, including queue throughput, missed contacts and utilisation trends
- **Role-based access:** Ensures secure, permission-based visibility and functionality for different user types, such as clinicians and administrators

Enabling secure integration with patient management systems and other approved applications, CLEO VWR also provides a version-controlled OpenAPI interface. This supports data exchange for queue status, reporting and operational workflows without requiring proprietary connectors.

2.6.5 API

We provide a secure, standards-based API that enables customers to integrate CLEO VWR functionality into their existing systems and workflows. Through the API, users can:

- Retrieve real-time queue status and access current patient queue positions and clinician availability
- Update queue configurations and adjust prioritisation rules, escalation settings and clinician pools
- Gather performance and reporting data, including metrics such as call volumes, wait times and utilisation for local BI tools
- Confirm patient engagement
- Query IVR confirmation status and patient readiness for consultation
- Export/download historical data and structured records for auditing, compliance and operational analysis

We secure all API interaction using TLS 1.2+ encryption and require authorised credentials. This API follows OpenAPI specification, providing clear documentation and version control for predictable integration.

2.6.6 Accessibility and usability

All interfaces are designed towards WCAG 2.2 AA standards. This includes our web-based interface, which is responsive and designed for ease of use by clinicians and administrators. CLEO VWR's accessibility and usability features include:

- Keyboard navigation support
- High-contrast mode
- Resizable text and responsive layout
- Clear, consistent User Interface (UI) design
- Screen reader compatibility
- Accessible documentation formats
- Error prevention and clear feedback
- Language clarity

2.6.7 Customisation

CLEO VWR offers flexible configurable options that allow users to tailor the service while remaining within a safe clinical framework. We have designed the following customisation elements to maintain simplicity while supporting local requirements:

- **Queue logic and prioritisation rules:** Define how patients are ordered, including escalation paths for urgent cases
- **Clinician pool configuration:** Adjust the number of clinicians assigned to queues and their availability settings
- **Call cadence and timing:** Configure when patients are contacted based on clinician throughput and service demand
- **IVR scripts and messaging:** Tailor patient communication prompts for clarity and compliance with local standards
- **Reporting dashboards:** Customise performance metrics and data views to support local Key Performance Indicators (KPIs) and governance needs
- **Integration settings:** Enable or disable API connections with patient management systems or other approved applications
- **Role-based permissions:** Configure user roles and access levels for clinicians, administrators and support staff

These options allow customers to adapt CLEO VWR to their unique environment without compromising clinical safety or system integrity.

2.6.8 Service levels and availability

The following Service Level Agreements (SLAs) define CLEO VWR's availability, response times and performance expectations under the G-Cloud 15 framework. To monitor system behaviour continuously, we review performance metrics with customers in quarterly account management meetings.

Metric	Target	How we measure it
Service availability	99.9%	Automated monitoring and uptime reporting
Priority 1 response time	1 hour	Recorded in Service Management Tool, allocated a Priority and customer receive case reference number
Priority 1 resolution time	4 hours	Request completion log
Priority 2 response time	2 hours	Recorded in Service Management Tool, allocated a Priority and customer receive case reference number
Priority 2 resolution time	16 hours	Request completion log

Priority 3 response time	8 hours	Recorded in Service Management Tool, allocated a Priority and customer receive case reference number
Priority 3 resolution time	5 business days	Request completion log
Priority 4 response time	8 hours	Recorded in Service Management Tool, allocated a Priority and customer receive case reference number
Priority 4 resolution time	30 business days	Request completion log

Figure 2.6.8.1: Our service levels and availability

To maintain these SLAs, we monitor CLEO VWR **24/7**, respond to critical alerts immediately and escalate risks to our Senior Management Team when required. If an outage occurs, we notify nominated contacts by email and publish updates through a service-status webpage. Full incident reports follow within agreed contract timeframes. We provide secure daily Single File Transfer Protocol (SFTP) data feeds and scheduled reports on queue and system usage, with additional metrics available on request.

3 G-Cloud alignment information

3.1 Section introduction

To support safe and efficient queue continuity and patient flow, we deliver CLEO VWR through a structured, collaborative delivery model. To achieve this, we combine defined project controls with flexible engagement, allowing us to meet the needs of diverse clinical environments. Our approach ensures clarity, accountability and strong governance from contract signature to service closure. This section explains how we work with buyer teams during onboarding, configuration, go-live, live-service operation and secure offboarding.

3.2 Onboarding and offboarding processes

For safe, controlled transitions in and out of service, we design onboarding and offboarding processes to give customers confidence and maintain compliance. Our onboarding approach has been developed to provide a structured and predictable process which aligns with NHS governance requirements. For offboarding, our approach provides full data portability, transparent activity, user control and zero vendor lock-in.

3.2.1 Onboarding

Reducing implementation risk and accelerating adoption, to begin onboarding, we align objectives, confirm responsibilities and establish governance needed to deliver CLEO VWR safely. For a smooth transition, our onboarding process includes planning workshops, migration support for data and integrations and governance alignment. Leading users through this process will be our dedicated Project Manager. We guide buyers through a clear, step-by-step process that prepares clinical, technical and operational teams for a smooth transition to live use.

1. **Kick-off and scoping:** To establish shared expectations, we meet our customer's project and governance teams to confirm scope, timelines and success criteria
2. **Statement of Work (SOW):** To formalise delivery, we produce an SOW outlining deliverables, dependencies, risks and commercial teams
3. **Access and environment set up:** We configure the VWR environment in the private cloud and ensure HSCN connectivity and Smartcard access where required. Supporting safe operation, we set up queue logic, escalation rules and clinician pools and agree IVR scripts and patient communication workflows with the customer
4. **Resource allocation and scheduling:** Ensuring clear accountability, we assign delivery roles, agree schedules and document milestones in the project plan
5. **Discovery and requirements confirmation:** Confirming readiness, we run technical and clinical workshops to validate requirements and align processes, including formulary configuration and reporting needs. Furthering this, we facilitate As-Is and To-Be mapping with NHS England
6. **Training and User Acceptance Training (UAT) preparation:** We deliver Train-the-Trainer sessions and provide user guides and videos. Assuring readiness, we support UAT focused on queue management, clinician workflows and IVR confirmation. We also require the customer completes the DCB0160 clinical safety assessment in response to DCB0129 before go-live

We conclude onboarding once the user approves UAT, completes governance checks, including DCB01060 and confirms readiness for deployment and go-live. To ensure safe transition, CLEO Systems provides onsite or remote support during go-live, followed by a 2-week hyper care period before transition to BAU.

3.2.2 Offboarding

To prepare users for a secure, transparent exit, we deliver a controlled offboarding process. This returns all buyer data, removes access and allows services to end without disruption. Providing expert oversight of this process will be our Project Management Team.

1. **Project closure review:** Confirming completion, we meet with the user to review deliverables, capture lessons learned, assess performance metrics and gather feedback
2. **Documentation and handover:** Supporting continuity, we provide final configuration outputs, test records, training assets and any required technical documentation
3. **Knowledge transfer:** For user self-sufficiency, we deliver targeted handover sessions with their teams to explain operational workflows, outstanding actions and confirm their competency
4. **Access revocation and data return:** Protecting confidentiality, in line with our Cyber Essentials Plus certification and NHS DSPT compliance, we remove all CLEO Systems access and return data through secure SFTP in agreed CSV formats. Supporting governance, we delete retained data within 3 months and issue a certificate of deletion
5. **Post-engagement support:** Maintaining service continuity, we offer advisory or optimisation through additional SOWs where requested

3.3 Data

3.3.1 Data importing and exporting

Ensuring full data portability and avoiding vendor lock-in, CLEO VWR supports open, non-proprietary data formats for importing and exporting information.

- **Data importing:** For support during onboarding, users can import data using CSV or JSON formats. Enabling this, we process structured inputs through controlled ingestion steps defined during implementation. This approach helps users integrate queue and usage data with local governance systems
- **Data exporting during the contract:** For local reporting, we provide secure daily transfers of usage data through SFTP, enabling onward processing into BI formats. Simplifying monitoring, users receive structured outputs covering queue activity, audit fields and operational metrics
- **Data exporting at any time:** Maintaining transparency, we export all user data upon request in open formats, including CSV and JSON. Supporting interoperability, we structure exports to align with local data models and analytical needs
- **End-of-contract data extraction:** Supporting secure exits, we provide a full SFTP data package in the user's preferred format at contract end. Ensuring compliance with our Cyber Essentials Plus certification and the NHS DSPT, we delete supplier-side data **within 3 months** of providing the export and issue a certificate of deletion

3.3.2 Analytics

To help users monitor queue performance, track clinician usage and improve patient flow, CLEO VWR provides structured usage metrics. Supporting operational oversight, we provide metrics covering:

- Queue volumes and throughput
- Clinician utilisation such as time spent on calls and average consultations per hour
- Patient engagement such as IVR confirmation rates and missed contact statistics
- Wait time analysis such as average/maximum patient wait times
- Operation trends including patterns in call handling and escalation events

For integration with the customer's own Business Intelligence (BI) tools, we deliver metrics through:

- Secure daily SFTP data feeds
- Scheduled reports in agreed formats such as CSV, JSON and PDF
- Additional on-request extracts to support bespoke dashboards or analytics

3.3.3 Independence of resource

To ensure consistent performance, CLEO VWR isolates user environments and prevents cross-tenant interference. Safeguarding stability, we monitor resource usage and scale infrastructure to prevent conflict from other users. Maintaining performance, we use load-balanced servers and proactive capacity planning.

3.3.4 Public sector networks

CLEO VWR connects securely to the HSCN to support Smartcard authentication and ensure compliance with NHS governance requirements. Protecting patient confidentiality and operational integrity, all traffic follows NHS security standards. Through this, CLEO VWR provides compliant access for authorised users within NHS environments.

3.3.5 Data-in-transit protection

To protect all data exchanges, CLEO VWR uses strong TLS 1.2 or above encryption and secure network protocols through the allowance of user Virtual Private Network (VPN) or IPsec gateways. Preventing internal interception, we secure service-to-service communication using TLS1.2+, network segmentation and controlled Application Programming Interface (API) gateways.

3.3.6 Asset protection

To protect assets and data, we host all data within UK-based private-cloud infrastructure and backed up to separate, segregated cloud environments managed by Arcserve. For data at rest, we apply physical and logical access controls aligned with the Cloud Security Alliance Cloud Controls Matrix (CSA CCM) v3.0, encryption and isolate tenant environments. To sanitise data, we erase user data using explicit overwriting of storage before reallocation, ensuring it cannot be recovered. To sustainably dispose of equipment, we maintain CSA CCM v4.0-aligned hardware disposal procedures.

3.4 Availability and resilience

3.4.1 Guaranteed availability

To guarantee 99.9% service availability, we have designed CLEO VWR to remain available, resilient and stable at all times. To achieve this, we use controlled hosting, continuous monitoring and structured recovery processes that protect buyers from disruption. Assuming responsibility for overseeing CLEO VWR's guaranteed availability will be our Product Team.

To maintain our commitment of 99.9% service availability, we monitor all environments 24/7, receive automatic alerts for anomalies through our infrastructure and application monitoring tools and respond to incidents using defined escalation pathways in line with our incident management process. To prevent outages, we operate CLEO VWR within UK-based private-cloud infrastructure that uses load-balanced servers, isolated resources and secure replication. Protecting performance, we scale resources proactively and separate customer workloads to avoid cross-tenant impact. To guarantee continuity, we back up all data daily to immutable vault storage and replicate these backups to a segregated cloud environment by Arcserve. For rapid restoration in the unlikely event of disaster scenarios, we follow annually tested disaster-recovery procedures aligned with NHS DSPT and internal Business Continuity Plan controls.

In the event of a service down incident, we triage all incidents immediately and escalate critical issues to senior engineers using our ITIL-aligned process. To protect users during high-security events, we communicate updates immediately through email alerts and a service-status webpage. For transparency, when an outage occurs, we notify all nominated user contacts to provide clear information on:

- Services affected
- Severity

- Issue description
- Actions taken
- Next status update

In the unlikely event of a major incident, we follow up with a full report to users within the agreed contractual timeframe.

Supporting consistent service quality, we analyse incident outcomes and integrate improvements into future releases.

3.5 Governance

We deliver CLEO VWR through a robust governance framework that ensures safe, compliant and high-quality service delivery. To achieve this, we combine accredited management systems, structured oversight and continuous improvement processes aligned with NHS and UK Government standards. Demonstrating the strength of our governance procedures, we operate under the following certifications and standards:

- NHS DSPT compliance
- NHS Digital governance requirements (including DCB0129)
- Cyber Essentials Plus

To maintain control and clear accountability, our governance framework management structure includes:

- Data Protection Officer (DPO) who oversees GDPR compliance and DPIA activities
- Information Governance Officer, who provides assurance and escalation in line with NHS IG requirements

To manage risks, we maintain formal change-control processes, which we review annually through a Change Management Board. Furthering this, we update documented risk registers during service reviews, with regular vulnerability scanning and annual penetration testing conducted by CREST-approved providers.

For continuous improvement, we review performance, security and clinical-safety data through structured processes such as:

- Quarterly service reviews to assess performance trends, SLA adherence and customer feedback
- Quarterly internal audits to verify compliance with DSPT, Cyber Essentials Plus and internal security controls
- Annual external audits to validate DSPT and penetration-testing outcomes
- Root-cause analysis following significant incidents to prevent recurrence and strengthen resilience
- Release management reviews ensure new features maintain clinical safety and operational stability

We use the findings from these activities to update our policies, including staff training, refine processes and guide enhancements for CLEO VWR.

3.6 Security

Supporting safe patient flow, we embed security throughout CLEO VWR to protect patient data, maintain system and queue integrity/workflow and comply with UK public-sector standards. Demonstrating this, we combine accredited governance frameworks, continuous monitoring and defined assurance activities overseen by our Information Governance Team. Confirming that CLEO VWR is operated using audited, nationally recognised security practices, we align controls with Cyber Essentials Plus, NHS DSPT and DCB0129 clinical

safety standards. Evidencing strong control maturity, **our latest DSPT external audit reported 0 areas for improvement.**

3.6.1 Operational security

We maintain operational security through controlled change, continuous monitoring and structured incident response. For stability, we assess every change using a formal Change Control Form that records risks, security considerations and implementation details. A Change Management Board reviews all changes and approves safe deployment.

Protecting CLEO VWR users, we monitor threats using an enterprise Security Information and Event Management (SIEM) and Security Operations Centre (SOC) platform. We assess emerging risks through weekly security meetings and intelligence feeds, including NHS CareCERT advisories. We patch critical **vulnerabilities within 72 hours** and high-risk issues **within 14 days**, following NHS CareCERT guidance. Threats we monitor for include, but are not limited to:

- Failed logins
- Privilege escalation
- Suspicious network activity
- Baseline deviations

Ensuring high-risk incidents are escalated immediately, we conduct automated risk scoring and alert prioritisation to the on-call security team. We handle all incidents under documented triage, containment, eradication and recovery steps. We communicate progress through user-nominated contacts and issue post-incident reports within agreed timeframes. Following major incidents, we conduct root-cause analysis and corrective actions, feeding improvements back into monitoring rules, playbooks and release processes.

To safeguard operations, we integrate operational security within our Business Continuity Plan (BCP) and disaster-recovery procedures. To confirm readiness, the Information Governance Team conducts annual BCP reviews, with any lessons learned from exercises and real events incorporated into our operations.

3.6.2 Staff security

Assuring users that systems are authorised correctly, we only grant access to vetted, authorised staff under least-privilege principles. For example, we screen personnel with access to system or patient data to BS7858 standards before access is granted.

3.6.3 Secure development

Managing supply chain risk, we develop CLEO VWR using a secure Software Development Life Cycle (SDLC) that includes threat modelling, peer code review, secure coding standards and dependency scanning. Security assurances we provide also include annual penetration testing by CREST-approved providers, continuous vulnerability scanning and remediation tracking. Through these processes, we confirm that we align with the UK Government Software Security Code of Practice.

3.6.4 Identity and authentication

CLEO VWR ensures only authorised clinicians and administrators can access functions that affect patient flow and operational safety. To achieve this, we apply the following restrictions and safeguards:

- Clinician access uses NHS Smartcards through Identity Agent V2+, aligning with NHS policy for secure authentication
- CLEO VWR applies role-based access controls to ensure users only access functions appropriate to their role, such as queue management and reporting

- Management access is restricted to named administrative users, with privileged activities logged and reviewed
- Customer Portal access requires username and password for approved user contacts, managed by the organisation's nominated administrators

3.7 Auditing

To ensure transparency, accountability and compliance with NHS and UK public-sector information-governance standards, CLEO VWR embeds comprehensive auditing across all environments. We record all user activity, including authentication attempts, queue management events, call handling events and administrative configuration changes, within secure logs. Ensuring full traceability, we also log all supplier actions performed on behalf of customers.

We securely store audit data within UK-based private-cloud infrastructure and protect it through strict access controls. We retain logs in accordance with customer-defined retention requirements, which can be exported in open formats (such as CSV or JSON) for clinical-safety reviews, regulatory audits or internal investigations. Customers may request extracts through the CLEO Systems Service Desk or receive scheduled reports as part of business-as-usual operations.

These auditing capabilities support effective queue and patient management, assist with incident investigation and underpin compliance with **Cyber Essentials Plus** and the **NHS DSPT**. Our most recent DSPT external audit reported **zero areas for improvement**.

3.7.1 Performance monitoring and metrics

To oversee CLEO VWR performance, our Live Service Monitoring, Technical Response and Account Management teams maintain responsibility for reviewing and improving performance. Identifying emerging issues early, this includes reviewing queue management action volumes, authentication events, patient communication events, escalation/prioritisation changes and general system behaviour.

Customers receive operational and usage metrics through secure daily SFTP data feeds and scheduled reporting. This enables them to integrate queue/patient management and activity data into their local governance processes or business intelligence systems. Additional or bespoke reporting is available on request.

To support optimisation, trend analysis and service development planning, we review insights from monitoring with customers during scheduled account management meetings. Ensuring timely investigation and resolution, performance deviations follow defined escalation routes, as defined in **Figure 2.5.1.1**. Enabling rapid intervention if performance degradation is detected, our monitoring systems generate alerts for infrastructure components, authentication services and application-level behaviour.

3.7.2 Compliance and quality management

Confirming the quality of our service, we maintain recognised industry standards and accreditations to deliver CLEO VWR safely, securely and consistently. Demonstrating our commitment to secure operations and strong information governance, we hold **Cyber Essentials Plus** and comply with the NHS DSPT. Furthering this, our infrastructure operations are accredited to and, as part of the IC24 Group, we hold the **Social Enterprise Gold Mark** and maintain compliance with the UK Government's ESOS scheme.

Our governance specialists, clinical-safety personnel and information-security teams manage compliance throughout our service's lifecycle. Protecting service stability, we apply structured service management processes to maintain quality, including controlled incident handling, defined change-management procedures and routine problem-management reviews. Our teams conduct scheduled penetration testing,

vulnerability scanning and internal audits to identify issues early. Findings from these reviews feed directly into our improvement actions.

We provide full traceability of these processes to maintain configuration integrity, track service changes and store audit evidence. We retain audit and compliance records for durations defined by each customer, supporting local governance and assurance activities. We review performance data, customer feedback and audit findings regularly. These reviews help us identify improvements, agree on corrective actions and maintain consistent quality across all environments.

3.8 Backup, restore and disaster recovery

Protecting service continuity and safeguarding patient-identifiable data, we maintain a comprehensive, multi-layered backup, restore and disaster-recovery framework for CLEO VWR. To do this, we combine secure immutable storage, segregated replication, robust governance controls and validated recovery procedures aligned with NHS DSPT expectations. Overseeing this will be our Information Governance Team.

Backup and replication

To protect data from corruption, accidental deletion or cyber-threats, we back up all CLEO VWR servers and databases daily to a secure, immutable vault, ensuring backups cannot be altered or overwritten. Strengthening resilience further, we replicate all backups to a separate, segregated cloud environment hosted and managed by Arcserve, providing physical and logical separation from the production platform. Our Infrastructure Team verifies the successful completion of each backup and monitors for anomalies. To protect retention compliance, with all backup data retained within UK-based cloud regions.

Objectives and governance

CLEO VWR maintains a **Recovery Point Objective (RPO) of 24 hours** and a **Recovery Time Objective (RTO) of ~2 hours**. To meet these objectives, we operate a suite of disaster-recovery, incident-response, data-breach and IG-incident plans that define decision pathways, activation triggers, communication flows and escalation responsibilities. Maintaining readiness, our BCP outlines the operational processes we follow during disruptive events, including technology failover, communication routes, team coordination, access controls and restoration sequencing. To ensure alignment with NHS expectations, we test and review the Business Continuity Plan annually, using outcomes to refine procedures and strengthen our recovery approach.

Restoration and assurance

To validate recoverability, we perform regular restoration activities, including controlled drills, database roll-forward checks and system validation testing. Minimising disruption, we maintain documented restoration steps, fallback procedures and prioritised recovery tasks that confirm mission-critical CLEO VWR functions are restored in the correct sequence. To strengthen reliability, we compare restoration outcomes against RPO/RTO targets and adjust technical configurations if performance gaps are identified. Following any continuity event or test exercise, we conduct a post-event review with technical, governance and operational leads. To improve resilience further, we integrate findings into updated procedures and adjust failover processes, communication steps and resource assignments.

End-to-end continuity alignment

To maintain oversight, senior leadership receives reports on disaster-recovery outcomes, readiness testing, identified risks and improvement activity. Ensuring transparency, CLEO Systems shares relevant continuity documentation with buyers upon request and provides assurance that restoration pathways and data recovery activities remain effective.

3.9 Training

CLEO VWR training is designed to ensure clinicians and administrators can use the system safely, confidently and in alignment with NHS standards. Our training supports local capability by building and ensuring smooth adoption during onboarding and go-live.

Training approach

Supporting an efficient rollout, we follow a Train-the-Trainer model, enabling local super-users to cascade training across teams at scale. Super-users receive detailed instructions on queue management workflows, clinician call handling, patient flow and reporting. This helps organisations build internal capability and reduce long-term dependency on external support. Ensuring familiarity with key workflows and system navigation, we deliver this training ahead of UAT.



Figure 3.9.1: Our training materials infographic

These materials support formal training sessions and act as long-term reference tools for end users and administrators and are updated following major releases.

Go-live and ongoing support

We align training with the customer's implementation schedule to support readiness for UAT and go-live. Additional sessions or refresher training can be provided upon request, using SFIA rates where required.

3.10 Service pricing

CLEO VWR pricing is bespoke and fixed to the user's needs, covering licenses, implementation, hosting, managed service, training, SMS messaging and connector costs as required. We price additional services using the SFIA rate card. Please refer to our CLEO VWR pricing document for further details.

3.11 Invoicing process

CLEO Systems invoices annually in advance on contract signature, with 30-day payment terms. We accept standard public-sector payment methods and align with government invoicing practices.

3.12 Termination terms

The minimum contract term for CLEO VWR is 12 months. Customers may end the Call-Off by giving 30 days' written notice, with CLEO Systems ceasing service on the agreed date and customers settling outstanding sums by the termination date. We return all data through SFTP in CSV (or JSON where requested), with supplier-side data deleted within 3 months and a certificate of deletion provided.

4 Security and data governance

4.1 Data protection and encryption

To protect sensitive data, we encrypt all data in transit using TLS 1.2 or above encryption. Where required, user-to-supplier traffic can be further protected through VPNs or IPsec. Enforcing strong authentication and access control, we also encrypt internal service and microservice communication and route through segmented networks with secure API gateways.

4.2 Data at rest, storage locations and physical security

We only store CLEO VWR within UK-based private-cloud infrastructure. We encrypt data using SQL Server TDE Encryption at rest through physical and logical access controls and tenant isolation. All CLEO Databases reside in our Database Servers in Norwich and Ashford. We align our datacentre security and asset controls with the CSA CCM. To comply with industry recognised standards, we are currently working towards aligning these processes with the latest CCM v4.0 controls.

4.3 Data sanitisation and disposal

Ensuring deleted data cannot be recovered, we sanitise data using explicit overwriting of storage before reallocation. Where equipment reaches end-of-life, we dispose of it in accordance with recognised standards, such as CSA CCM and ISO27001 and provide certificates of destruction on request.

4.4 Security testing and assurance

We provide assurance of the security of our systems through annual penetration testing by CREST-approved or Tigerscheme-qualified providers and continuous vulnerability scanning across environments. For transparency and auditability, we track findings from identification to remediation, with status reported through service governance and account management engagements.

4.5 Incident and protective monitoring management

To protect CLEO VWR from security threats and ensure safe clinical operation, we maintain continuous protective monitoring supported by our enterprise SIEM and SOC. Furthering this, we maintain a structured incident response approach aligned with ISO27035, Cyber Essentials Plus and the NHS DSPT.

- ✓ **Protective monitoring:** We operate 24/7 SIEM and SOC monitoring across CLEO VWR infrastructure, which analyses logs from servers, applications, authentication services and network controls. We escalate alerts for unusual or high-risk activity to our security specialists for investigation
- ✓ **Incident response:** We follow a formal incident response process that includes identifying, assessing and containing threats before restoring normal service. Aligning our processes with recognised NHS and UK Government standards, we escalate high-severity incidents immediately to senior security leaders
- ✓ **Preventative controls:** Minimising risk, we conduct annual penetration testing through CREST or Tigerscheme-approved providers, operate continuous vulnerability scanning and apply risk-based patching following NHS CareCERT guidance
- ✓ **Customer communication:** In the unlikely event of a major incident, we notify nominated customer contacts promptly and provide updates through agreed communication channels. We then issue a post-incident report in line with contractual requirements
- ✓ **Continuous improvement:** Our Governance Teams review lessons learned from incidents and security events, using them to strengthen monitoring rules, access controls and security

4.6 Configuration and change management

For performance stability, we track configuration items throughout their lifecycle in a Configuration Management Database. Before each release, we assess risk by performing security impact reviews for every change. To authorise updates, our Change Management Board approves deployments and rollback plans. Minimising disruption, we issue full incident reports within the contractually agreed timeframe.

4.7 Information security management and certifications

Managing all information security management procedures for CLEO VWR will be our Information Governance Team. Demonstrating our competence, we hold the following certifications:

- Cyber Essentials Plus
- Compliance with the NHS DSPT

To confirm our compliance, we undergo annual external audits to renew our certifications.

4.8 Secure development and cryptography

We follow secure development practices aligned to recognised standards on a self-assessed basis.

4.9 Identity and access management

We control access to CLEO VWR through strict authentication processes that ensure only authorised users can access patient data as defined by national NHS services. Users authenticate with NHS Smartcards through Identity Agent V2+, with all permissions enforced through CIS2 Role-Based Access Controls. We restrict administrative access to named users, protecting this through standard username and password authentication. We log all privileged activity for auditing purposes. CLEO VWR does not use multi-factor authentication, single sign-on, Security Assertion Markup Language (SAML) or Open Authorisation 2.0.

5 Supplier information

5.1 About us

We are CLEO Systems, a UK health-tech provider within the IC24 Group, delivering intuitive digital solutions that simplify queue and patient management and improve clinical workflows. Founded in 2019 in Ashford, Kent, we operate as part of a social enterprise, reinvesting surplus to strengthen care quality and support sustainable NHS innovation. We are a specialist organisation with in-house clinicians and digital experts who support product development, testing and iterative improvement across multiple NHS environments.

Demonstrating improved clinician efficiency, through CLEO VWR has saved 460+ clinician hours per month for our existing customers.

Supporting safe, efficient clinical and patient management, we serve key sectors across the NHS, including:

- Secondary care outpatients
- Community services
- Urgent care
- Community pharmacies

Our organisational mission is to empower clinicians, improve patient experience and increase efficiency through intuitive, clinically informed system design. We use these key values to shape how we plan, deliver and support all our innovative solutions. We maintain recognised governance and security standards, as evidenced by our accreditations as shown below:

- Cyber Essentials Plus
- Compliance with the NHS DSPT and NHS Digital

5.2 CLEO VWR development and rationale

Origin and purpose

We conceived CLEO VWR through a joint innovation initiative between Urgent Health UK and the Innovation Department at the University of Warwick. As a group, we focused on reducing operational friction in urgent care. We wanted to address the core problem of clinicians spending time dialling patients and chasing unanswered calls, which caused delays, lower throughput and a poor patient experience.

Concept to capability

Our team identified The Waiting Room (originally developed by Ummanu) as a proven approach. Early NHS pilots showed clinicians doubled their productivity with virtualised queuing and automated outreach, going from 1.5 to 3+ consultations per hour. With Ummanu signalling a market exit, we acted to safeguard continuity for the NHS, acquiring the technology, bringing the team on board and integrating the capability into the CLEO product suite.

5.3 How to buy

CLEO VWR can be procured directly through the CCS G-Cloud 15 Digital Marketplace. Customers can search for CLEO Systems on the Digital Marketplace and select the required service listing. Once selected, the customer and CLEO Systems will:

1. Agree a SOW detailing scope, deliverables, timescales and pricing
2. Raise a Call-Off Contract under the G-Cloud framework terms
3. Issue a Purchase Order to confirm commencement

Ensuring transparency and compliance with public-sector procurement regulations, all engagements are delivered in line with G-Cloud framework conditions.

For any enquiries, please contact:

hello@cleosystems.com
03333 200024