G-Cloud 15 (RM1557.15)

CLEO Systems 24 LTD

CLEO EPS
Service Definition

January 2026

Table of contents

1 Introduction

1.1 Document structure

This Service Definition outlines how CLEO Electronic Prescribing Solution (EPS) 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 EPS
- **Section 2 – Service description:** Describes what CLEO EPS 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 EPS 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 EPS 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 EPS 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 EPS. It can be used to:

- Assess service suitability with Section 2 summarising what CLEO EPS does, the settings it supports and the problems it solves, helping alignment with local digital prescribing 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 Systems provides secure, clinically aligned digital prescribing services designed to support NHS organisations across outpatient and community settings. Founded in 2019 in Ashford, Kent, we operate as a UK-based subsidiary of the IC24 Group, giving customers confidence in our healthcare expertise and long-standing commitment to public-sector delivery.

Reducing delays, strengthening safety and patient access, our CLEO EPS service replaces handwritten FP10s with a digital, Spine-connected workflow. This service currently supports over **30+ NHS Trusts**, community services and independent healthcare providers seeking safer, faster and more sustainable prescribing pathways. Aligning directly with UK Government expectations, CLEO EPS also helps organisations address national priorities, including:

- Reducing paper usage
- Improving sustainability
- Enhancing prescription security
- Supporting more remote consultation models

These outcomes support wider transformation programmes across the healthcare sector in the UK, including remote consultation pathways and outpatient redesign.

We shape our approach through our in-house clinicians, verifying that our service remains intuitive, clinically safe and grounded in real operational practice. Providing data protection and system integrity assurance, we hold **Cyber Essentials Plus** certification and comply with the NHS Digital Data Security and Protection Toolkit (NHS DSPT).

Offering a practical route for organisations seeking a low-disruption, high-impact prescribing solution, CLEO EPS combines simplicity, fast adoption and proven safety. Under the G-Cloud 15 Framework, we provide a trusted, scalable service that helps clinical teams work more efficiently to deliver better experiences for patients.

2.2 Delivery framework

We deliver CLEO EPS through a structured, clinically informed delivery framework designed to provide a safe, predictable and efficient transition from paper-based prescribing to digital workflows. Ensuring consistency across all implementations, our approach supports buyers from initial mobilisation through configuration, training, testing, go-live and ongoing optimisation.

Our delivery lifecycle combines clinical engagement, technical readiness and robust governance. We begin by confirming service scope, data requirements and user roles, before configuring the environment, providing targeted training and supporting end-to-end testing. Once live, we deliver a short period of enhanced support before transferring the service to business-as-usual operation, supported by our Service Desk, Account Management Team and continuous improvement processes.

We designed our delivery framework this way to minimise disruption, accelerate adoption and ensure clinical safety at every stage. We underpin each phase with defined responsibilities, transparent communication and alignment with NHS digital-safety standards. This enables our customers to adopt CLEO EPS quickly, reduce operational risk and achieve measurable benefits from the outset.

Our visual delivery framework and lifecycle diagram:

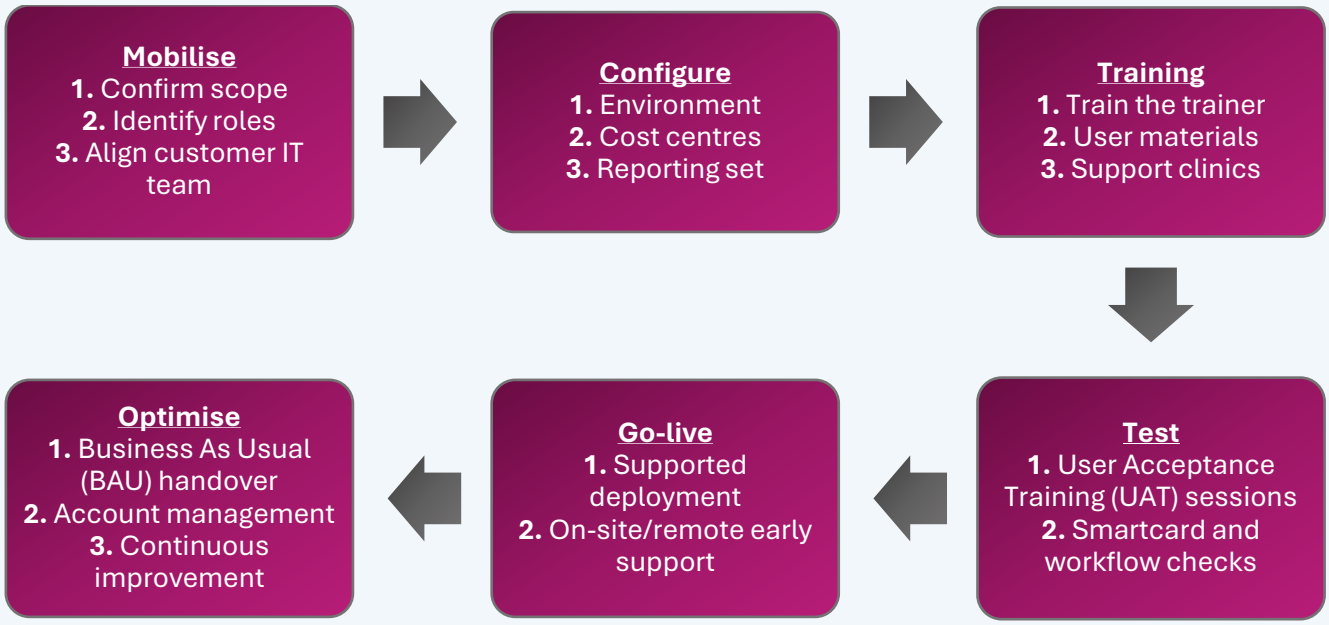

Figure 2.2.1: **Our visual delivery lifecycle diagram**

2.3 Service features / benefits

Our CLEO EPS service provides the following features:

- **Spine-connected electronic prescribing:** CLEO EPS connects securely to the NHS Spine to enable electronic prescription transfers to any community pharmacy
- **Standalone, no-integration deployment model:** CLEO EPS operates independently of existing EPR or PAS systems, requiring no technical integration
- **NHS Smartcard authentication/Role-Based Access Control (RBAC):** Clinicians authenticate using their NHS Smartcard roles, ensuring role-appropriate prescribing functions
- **Robust patient-search function:** CLEO EPS uses NHS demographic search criteria and prescription IDs to match patients accurately
- **Pharmacy search and digital routing:** Clinicians can select from nearby pharmacies and send prescriptions electronically through the NHS Spine
- **Multiple cost-centre and finance support:** Our service supports multiple cost centres, enabling efficient budget allocation and departmental reporting
- **Structured digital audit and reporting outputs:** CLEO EPS provides prescriber-level reporting and a secure daily data feed for local business intelligence
- **Configurable formularies and clinical warnings:** Local formularies and prescribing guidance can be configured to support consistent, safe clinical decision-making
- **SMS prescription notifications:** CLEO EPS can send SMS messages confirming prescription details to patients
- **Remote-consultation capability:** Our solution supports prescribing during remote consultations, enabling safe electronic workflows without face-to-face contact

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

Reduced travel, carbon emissions and improved sustainability, removing the need for patients and clinicians to travel to collect, post or deliver FP10s

Improved prescription security by eliminating risks linked to lost or stolen FP10 pads, with prescriptions tracked through controlled, auditable processes

Fewer prescribing errors, enhanced patient safety and delay reduction through structured workflows which reduce illegibility errors and improve clarity

Faster end-to-end prescribing process as clinicians complete and send prescriptions within minutes, freeing time for direct patient care and shortening wait times

Increased capacity for clinical teams through the reduction of administrative tasks such as postage, printing and FP10 management

Clearer and more effective governance and reporting as daily data feeds and prescriber-level reporting enables more informed medicines-management decisions

Lower operational costs through reductions in stationery, printing, posting and administrative activity expenditure creating recurrent savings

Improved patient experience and equity as they can choose any convenient community pharmacy and collect medication without visiting clinical sites

Reduced paper use and waste with electronic workflows removing reliance on paper FP10 pads to support wider environmental objectives

2.4 Service scope

CLEO EPS is a Software-as-a-Software (SaaS) prescribing solution delivered as a private-cloud service, designed to support NHS outpatient and community-based clinical teams. To optimise implementation and ensure compliance, we define the scope of CLEO EPS through 4 elements:

- Service characteristics
- Add-ons and extensions
- Cloud deployment model
- Operational constraints and system requirements

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

2.4.1 Add-ons and extensions

CLEO EPS is not an add-on or extension to another software service and is a standalone service.

2.4.2 Cloud deployment model

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

- Ensure data remains full sovereign by hosting all components within UK-based private cloud infrastructure
- Protect performance and support safe prescribing 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

1. Technical and environmental constraints

- **Smartcard authentication must be available**, using NHS Identity Agent V2.4.10.0+ or above
- **Windows devices** meet the minimum specifications outlined in Section 2.6.4
- **Health and Social Care Network (HSCN) connectivity** must be available at all prescribing locations
- **Oberthur middleware** must be installed for Smartcard use
- **NHS Credential Management v1.4.2.0+** must be installed where FHIR messaging is enabled

2. External dependencies

- **NHS Spine** for prescription transmission
- **Personal Demographics Service (PDS)** for patient demographics
- **GP Connect** for document delivery
- **FDB Multilex or the NHS Dictionary of Medicines and Devices (DM+D)** for medicines information

3. Maintenance windows

- We schedule planned maintenance **outside core support hours (08:00-18:00, Mon-Fri)**
- We notify customers of maintenance in advance through the Service Desk or Customer Portal
- Critical updates may require accelerated deployment to maintain clinical safety

4. Geographic and performance considerations

- CLEO EPS is designed for UK-based use only, as it depends on HSCN and NHS national services
- Performance may reduce outside the UK due to the absence of HSCN routing

2.4.4 System requirements

Requirement	Details
Operating system	Windows 10 or later
Processor	Dual-core 2GHz or faster
Memory	Minimum 450MB dedicated per user
Install space	450MB
Display	Optimal 1920x1080 resolution
Frameworks	.NET Framework 4.8
NHS Identity	NHS Digital Identity Agent V2.4.10.0+, SessionLockPersistence_Disabled
Middleware	Oberthur (for Smartcard use)
Smartcard drivers	PV mini-driver for series 9 cards
Credential management	NHS Credential Management v1.4.2.0+
Connectivity	HSCN connection

Additional components	Microsoft Visual C++ 2019 Redistributable, up-to-date Intel graphics drivers
Third-party system requirements	• NHS Spine applications • PDS • GP Connect APIs • FDB Multilex or DM+D data sources
Browser requirements	• CLEO EPS does not run in a browser • All prescribing is delivered by a Windows desktop client
Network requirements	• Stable HSCN access • Firewalls configured to allow national NHS service endpoints

Figure 2.4.4.1: **CLEO EPS system requirements**

2.5 User support

To help users resolve issues quickly and maintain safe prescribing, 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**, providing updates accordingly.

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 below escalation model 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.

2.6 How users work with our service

2.6.1 Browsers

CLEO EPS does not operate in a web browser. Providing consistent performance, secure Smartcard authentication and full compliance with the NHS Spine, our service uses a Windows desktop application.

2.6.2 Desktop application

CLEO EPS uses a dedicated Windows desktop application to support safe, responsive prescribing. To achieve this, CLEO supply the CLEO EPS MSI for the customer to install on approved devices through the customer's endpoint-management tools, whilst CLEO undertake the implementation of the backend services and databases. Key characteristics of our desktop application include:

- Runs on Windows 10 or later
- Uses NHS Smartcard authentication through Identity Agent V2.4.10.0+
- Supports clinical workflows requiring Spine connectivity
- Deploys centrally to reduce local configuration effort

2.6.3 Mobile

CLEO EPS is not designed for use on mobile devices.

2.6.4 Service interface

To support efficient clinical use, we design the CLEO EPS interface around clarity, safety and ease of navigation. Our interface features include:

- Simple, task-focused workflows
- Structured patient-search screens using NHS-recognised criteria
- Configurable formularies and prescribing warnings
- Clear, step-by-step prescribing pathways
- Consistent User Interface (UI) components that reduce training effort

2.6.5 API

CLEO EPS provides incoming APIs to support integration with approved NHS services and local systems. A test environment is available for buyers, with API documentation provided in PDF format. Through the API, users can:

- Receive structured clinical messages using FHIR standards
- Support GP Connect Send Document flows
- Enable reporting and prescribing insights through controlled data feeds
- Integrate securely with local BI tools

2.6.6 Accessibility and usability

All interfaces are designed towards WCAG 2.2 AA standards. Features include keyboard navigation, screen-reader compatibility, high-contrast modes and scalable text.

2.6.7 Customisation

CLEO EPS provides configurable options that allow users to tailor the service while remaining within a safe clinical framework. For example, users can customise the following configurable elements:

- Local formularies and prescribing guidance
- Dose-string translations and prescribing warnings
- Cost-centre configurations for financial tracking
- User setup and role-based permissions
- Reporting data feeds aligned to local BI needs

We offer customisation to user administrators to configure user access, cost centres and some formulary components, with CLEO Systems configuring advanced/account-level settings. This includes integrations and feature enablement.

2.6.8 Service levels and availability

The following Service Level Agreements (SLAs) define CLEO EPS' 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 with the customer receiving 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 with the customer receiving 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 with the customer receiving 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 with the customer receiving 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 EPS **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 prescribing and system usage, with additional metrics available on request.

3 G-Cloud alignment information

3.1 Section introduction

To support safe and efficient prescribing, we deliver CLEO EPS 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 buyers 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 EPS safely. Leading users through this process will be a 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. **Quote:** To formalise delivery, we produce a quote outlining deliverables, dependencies, risks and commercial teams
3. **Access and environment set up:** To enable authentication, our customer prepares Smartcards and assigns the required Roles and Activities (portal requirement). Maintaining security, we ensure the customer has HSCN connectivity and installs Oberthur middleware and Identity Agent V2.4.10.0+ on devices. Supporting deployment, the customer's IT team deploys the CLEO EPS MSI package to approved devices
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:** Preparing a safe rollout, we deliver Train the Trainer sessions and supply user guides and videos in PDF and MP4 formats respectively. Assuring readiness, users conduct UAT in either a dedicated test environment or the live environment with test patients. After UAT, we require users to complete the DCB0160 clinical risk assessment to legally certify that the new IT system is safe for live patient care

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 2 weeks of early-implementation support before transferring to business as usual.

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 quotes where requested

3.3 Data

3.3.1 Data importing and exporting

Ensuring full data portability and avoiding vendor lock-in, CLEO EPS 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 prescribing data with local governance systems
- **Data exporting during the contract:** For local reporting, we provide secure daily transfers of prescribing and usage data through SFTP, enabling onward processing into BI formats. Simplifying monitoring, users receive structured outputs covering prescribing 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 prescribing activity, track performance and strengthen medicines-management governance, CLEO EPS provides structured usage metrics. Supporting oversight, we provide metrics covering:

- Prescribing volume
- Authentication events
- Transaction throughput
- Performance statistics
- Operational usage patterns

For local BI strategies, we deliver metrics through:

- Secure daily SFTP data feeds
- Scheduled reports
- Additional on-request extracts

3.3.3 Independence of resource

To ensure consistent performance, CLEO EPS 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 EPS connects securely to the HSCN to support Smartcard authentication, Spine access and national interoperability. Enabling connectivity, users ensure HSCN access at prescribing locations. Protecting safety, all traffic follows NHS governance requirements. Through this, we provide compliant access to NHS Digital services including:

- NHS Spine
- PDS
- GP Connect
- CIS2 authentication

3.3.5 Data-in-transit protection

To protect all data exchanges, CLEO EPS 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 developed 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 EPS 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 EPS' guaranteed availability will be the CLEO Service Desk Manager.

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. To prevent outages, we operate CLEO EPS 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 EPS 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
- EMIS accredited partner
- NHS Digital
- 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 EPS.

3.6 Security

We embed security throughout CLEO EPS to protect patient data, maintain system integrity 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 EPS is operated using audited, nationally recognised security practices, we align controls with Cyber Essentials Plus and the NHS DSPT. 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 EPS 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 includes but is 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, our Governance Officer 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 EPS 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 EPS ensures only authorised prescribers and administrators can access functions that affect patient safety. To achieve this, we apply the following restrictions and safeguards:

- Prescriber access uses NHS Smartcards via Identity Agent V2.4.10.0+ with the configuration setting SessionLockPersistence_Enabled = false, aligning with NHS policy
- CLEO EPS performs CIS2 RBAC checks to verify nationally defined Roles and Business Functions before enabling prescribing actions
- Restrict management access to named administrative users, with privileged activities logged and reviewed
- Customer Portal access requires username and password for approved user contacts, which is managed by the user's nominated administrators

3.7 Auditing

To ensure transparency, accountability and compliance with NHS and UK public-sector information-governance standards, CLEO EPS embeds comprehensive auditing across all environments. We record all user activity, including authentication attempts, prescribing 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 safe prescribing, 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 EPS 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 prescribing volumes, authentication events, transaction throughput and general system behaviour.

Customers receive operational and usage metrics through secure daily SFTP data feeds and scheduled reporting. This enables them to integrate prescribing 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 EPS 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, we

infrastructure operations are accredited toas 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 corrective actions and maintain consistent quality across all environments.

3.8 Backup, restore & disaster recovery

Protecting service continuity and safeguarding patient-identifiable data, we maintain a comprehensive, multi-layered backup, restore and disaster-recovery framework for CLEO EPS. 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 EPS 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 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 EPS maintains a **Recovery Point Objective (RPO) of 24 hours** and a **Recovery Time Objective (RTO) of 1 hour** for CLEO EPS. 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 EPS 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 EPS 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 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 instruction on prescribing workflows, Smartcard authentication, patient search, formulary usage, clinical warnings, cost-centre allocation and pharmacy routing. 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 EPS 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.

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 EPS 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 EPS 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 EPS 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 EPS 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 configurations

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 EPS 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 EPS 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 V2.4.10.0+, 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 EPS 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 prescribing 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 clinical safety, secure patient data transfer and readiness for busy outpatient and community environments, CLEO EPS achieved NHS Digital accreditation in 2022.

Supporting safe prescribing and efficient 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 of our innovative solutions. We maintain recognised governance and security standards, as evidenced by our accreditations shown below:

- Cyber Essentials Plus
- NHS DSPT
- NHS Digital

Through our **6+ years of experience**, we have delivered digital transformation across NHS Trusts, helping them to reduce administrative burden, strengthen prescription security and support more sustainable service models.

- Whittington Health NHS Trust
- Midlands Partnership University NHS Foundation Trust
- Ashford & St Peter's Hospitals NHS Foundation Trust

Evidencing our success with these clients, they provided the following testimonials:

"Traditionally, when community patients require medication, requests were often sent to GPs to issue prescriptions. With CLEO EPS, community teams can issue prescriptions directly and electronically, alleviating the burden on GPs."
Pharmacy Digital and Informatics Lead, Whittington Health NHS Trust

"Working with CLEO Systems and NHS Digital, we have tailored EPS to suit different service requirements, ensuring benefits such as reduction in travel, postage and time, which are being realised by a wide variety of services across the Trust."
Head of Pharmacy Digital Improvement & Innovation, Midlands Partnership University NHS Foundation Trust

"Very knowledgeable team. Our Project Manager, James, has been very supportive and helpful throughout the project implementation."
Digital Matron, Ashford & St Peter's Hospitals NHS Foundation Trust

5.2 How to buy

CLEO EPS 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