

G-Cloud 15 (RM1557.15)

Klinik Healthcare Solutions Ltd

Lot 2b - Klinik Access

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 What the service delivers	5
2.3 Who uses the service	5
2.4 Delivery framework	6
2.5 Service features / benefits	7
2.6 Service scope	7
2.6.1 Add-ons and extensions	7
2.6.2 Cloud deployment model	7
2.6.3 Service constraints	7
2.6.4 System requirements	8
2.7 User support	8
2.7.1 Support details	8
2.7.2 Accessibility and usability	9
2.8 How users work with our service	9
2.8.1 Browsers	9
2.8.2 Desktop application	9
2.8.3 Mobile	10
2.8.4 Service interface	10
2.8.5 API	10
2.8.6 Accessibility and usability	10
2.8.7 Customisation	10
2.8.8 Service levels and availability	10
3 G-Cloud alignment information	12
3.1 Section introduction	12
3.2 Onboarding and offboarding processes	12
3.2.1 Onboarding	12
3.2.2 Offboarding	13
3.3 Data	14
3.3.1 Data importing and exporting	14
3.3.2 Analytics	14
3.3.3 Independence of resource	15
3.3.4 Public sector networks	15



3.3.5 Data-in-transit protection	15
3.3.6 Asset protection	15
3.4 Availability and resilience.....	16
3.5 Governance	16
3.6 Security	17
3.6.1 Operational security	17
3.6.2 Staff security.....	17
3.6.3 Secure development.....	17
3.6.4 Identity and authentication	18
3.7 Auditing.....	18
3.7.1 Performance monitoring and metrics.....	18
3.7.2 Compliance and quality management	19
3.8 Backup, restore & disaster recovery	19
3.9 Training	20
3.10 Service pricing	20
3.11 Invoicing process	21
3.12 Termination terms	21
4 Security and data governance	22
4.1 Data protection and encryption	22
4.2 Data at rest, storage locations, and physical security.....	22
4.3 Data sanitisation and disposal.....	22
4.4 Security testing and assurance	24
4.5 Incident and protective monitoring management	24
4.6 Configuration and change management.....	25
4.7 Information security management and certifications.....	25
4.8 Secure development and cryptography	25
4.9 Identity and access management.....	26
5 Supplier information.....	27
5.1 About us	27
5.2 Relevant experience and testimonials	28
5.4 How to buy.....	30

1 Introduction

1.1 Document structure

This service definition describes how Klinik Access works and how it is delivered to public sector buyers through the G-Cloud 15 framework. It is intended to provide clear, factual information to support NHS organisations in understanding the service, its operation and how it can be adopted within primary care settings.

The document explains what the service does, who it is for, how it is delivered and how it is supported throughout its lifecycle, including onboarding, day-to-day operation and end-of-contract arrangements.

This service definition is structured into 3 main sections:

1. Service description, covering what the Klinik Access is, who uses it and how it is delivered
2. Operational delivery and G-Cloud alignment, covering onboarding, support, security and service management
3. Supplier information, providing background information about Klinik and how the service can be procured through G-Cloud 15

1.2 How to use this document

This service definition is intended to support NHS buyers at each stage of the G-Cloud procurement process, from initial service evaluation through to contract award and service delivery:

- For early-stage evaluation, Section 2 (Service description) explains what Klinik Access is, who it is for and how it is delivered, helping buyers assess alignment with local primary care needs
- For due diligence and service planning, Section 3 (Operational delivery and G-Cloud alignment) sets out how the service is onboarded, supported and managed, including service levels, data management, security and exit arrangements
- For supplier context and procurement, Section 4 (Supplier information) provides background information about Klinik Healthcare Solutions and explains how the service can be procured through the G-Cloud 15 framework

This document is designed to be read alongside the Digital Marketplace service listing and supports informed decision-making throughout the lifecycle of the service.

2 Service description

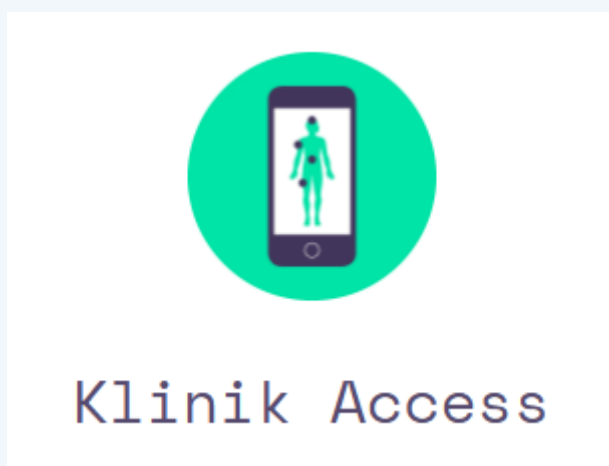
2.1 About our service

Klinik Access is a cloud-based digital triage and patient flow management service designed for NHS primary care. It is used by GP practices, Primary Care Networks (PCNs) and Integrated Care Boards (ICBs) to manage patient demand, improve access to care and support safe, efficient routing of patient enquiries.

The service provides a structured digital front door for patients to submit requests for care and advice. These requests are captured using clinically designed triage logic and are directed to the most appropriate care pathway or professional based on urgency, condition and local configuration. This supports practices to manage demand more effectively while maintaining clinical oversight.

Klinik Access is intended to support day-to-day primary care operations rather than replace clinical decision-making. It enables practices and networks to reduce administrative burden and make better use of the wider practice team, including non-GP roles.

The service is delivered as a fully managed Software as a Service (SaaS) solution, accessed through supported web browsers. It is hosted in the UK and designed to integrate with existing NHS primary care systems, supporting adoption without the need for local infrastructure or software installation.



2.2 What the service delivers

Klinik Access is an AI-powered triage and patient flow management solution for primary care, built by GPs and other healthcare professionals. The service enables patients to submit requests for care and advice through a digital front door, capturing relevant information at the point of contact and presenting it to practice teams in a consistent format.

Using configurable triage pathways and workflows, the service supports safe prioritisation of requests and routes them to the most appropriate care pathway, team or professional based on local configuration. This includes clinical review, non-clinical handling and onward routing where appropriate.

Practice staff can review and manage requests, communicate with patients, redirect cases internally and book appointments as part of a single workflow. At network level, the service supports shared or hub-based triage models, providing visibility of demand and activity across practices. To support operational planning, we provide dashboards that give insight into volumes, trends and service pressures.

2.3 Who uses the service

Klinik Access is used by a range of users within NHS primary care, each interacting with the service in different ways based on their role:



- **Patients** use the service to submit requests for care and advice through a structured digital front door. They can provide information about their symptoms or needs, upload supporting images where appropriate and receive messages or updates from the practice.
- **Practice staff** use the professional interface to review incoming requests, manage workflows and coordinate responses. This includes administrative staff, care navigators and clinical support staff who handle non-clinical and administrative enquiries or route requests to the appropriate team.
- **Clinicians**, including GPs and other clinical professionals, use the service to review and prioritise patient requests, make clinical decisions and communicate with patients as required. The service supports clinical oversight while reducing unnecessary administrative handling.
- **Primary Care Network (PCN)** and network teams use the service to support shared or hub-based triage models, enabling collaboration across practices and providing visibility of demand and activity at network level.

2.4 Delivery framework

Klinik Access is delivered as a fully managed Software as a Service (SaaS) solution. It is accessed through supported modern web browsers and does not require local software installation or specialist hardware. The service can be used on desktop, laptop, tablet and mobile devices. The service typically goes live within 2–4 weeks, depending on the agreed configuration and onboarding requirements.

To support seamless adoption within established workflows, Klinik Access is designed to integrate with existing NHS primary care systems. Our delivery process is described below:

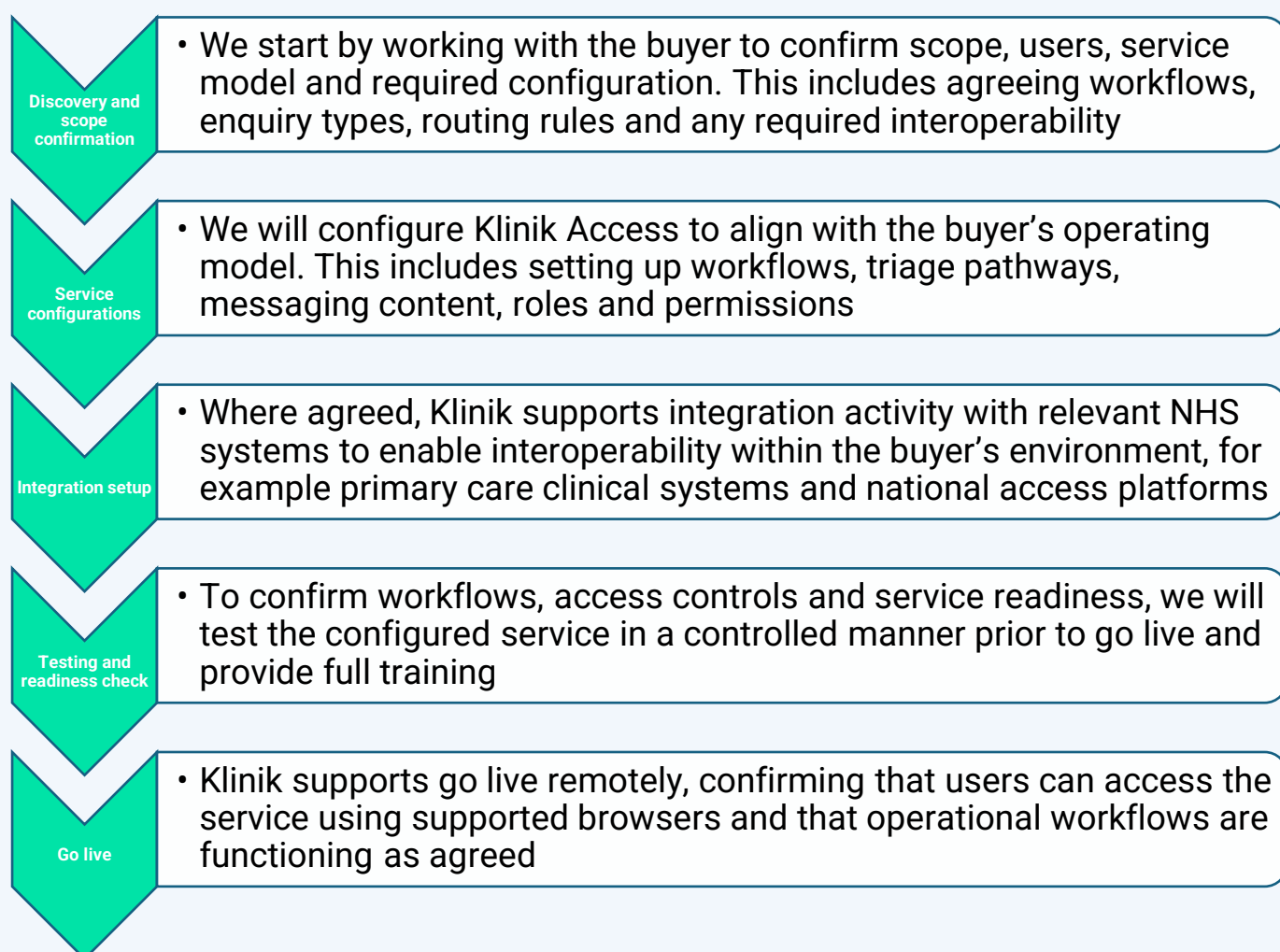


Figure 1: Our step-by-step delivery process

2.5 Service features / benefits

Klinik Access provides a structured approach to managing patient demand and access within NHS primary care. Its core features are designed to support safe triage, efficient patient flow and effective use of practice and network resources. Below, we have highlighted the main features of Klinik Access and the practical benefits our customers see as a result:

Service Feature	Benefit to NHS primary care organisations
Digital total triage platform supporting online and telephone access	Improves patient access by offering consistent digital and assisted routes into care
Dynamic symptom capture with structured questions and free-text input	Supports more complete patient history-taking at first contact
Hub-based triage capability across networks of practices	Enables scalable triage models across PCNs and ICBs
Configurable workflows linking enquiries to teams or resources	Aligns routing and handling with local operating models
Internal case redirection and collaboration tools	Supports efficient use of the wider practice team
Built-in two-way messaging between staff and patients	Reduces unnecessary follow-up and improves communication
Secure patient image upload linked to enquiries	Supports more informed triage where clinically appropriate
Automated routing based on urgency and presenting condition	Helps prioritise urgent cases and direct requests appropriately
Integrated appointment booking for patients and staff	Streamlines the journey from triage to appointment
Dashboards showing demand, frequency and prevalence metrics	Provides insight to support planning and capacity management

Figure 2: Main features and benefits of Klinik Access

2.6 Service scope

2.6.1 Add-ons and extensions

Klinik Access is a standalone service. It is not an add-on or extension to another product. The service is designed to operate independently while integrating with existing NHS primary care systems where required.

2.6.2 Cloud deployment model

Klinik Access is delivered using a public cloud deployment model. The service is hosted within a secure cloud environment located in the United Kingdom and is fully managed by Klinik. Buyers do not need to manage or provision any underlying infrastructure.

2.6.3 Service constraints

Klinik Access is delivered as a cloud-based SaaS solution and requires a stable internet connection. The service is accessed through supported modern web browsers and does not operate offline. Where temporary connectivity is lost, data entered is automatically synchronised once the connection is restored.

Onboarding, training and ongoing support are provided remotely. Configuration is required during onboarding to align workflows and triage pathways with local practice, PCN or ICB operating models. Planned maintenance is scheduled outside core UK primary care hours wherever possible and is communicated in advance.

2.6.4 System requirements

To ensure optimal performance, the service requires the following minimum system configuration:

Category	Requirement
Supported web browsers	- Google Chrome (version 144 or higher) - Microsoft Edge (Chromium-based, version 144 or higher) - Mozilla Firefox (version 136 or higher) - Apple Safari (version 18.3 or higher)
Supported operating systems	- Windows 10 (22H2) and Windows 11 (24H2) - macOS Sequoia version 15.5 or higher
Hardware	Modern desktop, laptop or mobile device capable of running supported browsers
Connectivity	Minimum internet speed of 1 Mbps required for reliable operation
Device security	Devices must have a software firewall enabled and receive regular security updates

Figure 3: System requirements for Klinik Access

2.7 User support

Klinik Access is designed to be intuitive and user friendly for both patients and practice teams, with support and interaction built into day-to-day use of the service. To ensure buyers can access help quickly, resolve issues efficiently and maintain continuity of operations, we provide a structured, responsive support service. We have aligned our support model to ITIL principles and we deliver this through a combination of self-service resources, multi-channel helpdesk support and escalation pathways to technical specialists.

2.7.1 Support details

To provide timely assistance while minimising disruption to primary care service, we provide support through a structured, remote support model. We deliver support through defined channels, with prioritisation and escalation based on incident severity:

- **Support channels:** Email support, phone support and an online ticketing system are provided
- **AI-driven self-service:** An AI-supported Knowledge Base is available to help users access guidance and documentation before contacting support
- **Support hours:** Standard support is available Monday to Friday, 08:00–17:00 UK time, excluding Bank Holidays
- **24/7 support:** 24/7 support is available for high-severity service incidents through defined escalation routes
- **Response times:** Support requests are prioritised by severity. High-severity incidents receive immediate response (within 8 hours at the latest), including evenings and weekends. Medium-severity requests are responded to within 1 working day. Low-severity requests are responded to within 5 working days
- **Weekend response:** Standard support operates during business hours. High-severity incidents are supported 24/7, including weekends and Bank Holidays
- **Support accessibility:** The online ticketing system meets WCAG 2.2 AA accessibility standards

- **Third-party support access:** Third parties engaged by the buyer (such as delivery partners or system suppliers) can access support where authorised by the buyer, using role-based access controls
- **Service management and escalation:** Support is delivered through the Klinik service desk, with escalation to senior technical staff and named contacts for high-severity incidents
- **Account management:** Named escalation contacts and a Service Manager are available for service-related issues and major incidents

2.7.2 Accessibility and usability

Klinik Access is designed to be accessible and usable for a wide range of users, including patients, clinicians and practice staff with differing access needs. Accessibility considerations are embedded into the design of both the patient-facing digital front door and the professional interface used by practice teams.

- The service interface is designed to meet WCAG 2.2 AA accessibility standards. This includes clear and consistent layouts, readable text, appropriate colour contrast, logical navigation and compatibility with keyboard navigation and screen reader technologies
- The responsive design ensures the service can be used effectively on desktop, tablet and mobile devices without loss of functionality
- For users who are unable to engage digitally, the service supports alternative access routes, such as telephone-based triage, ensuring inclusive access to primary care services
- Interface changes and new functionality are reviewed with accessibility in mind and accessibility checks form part of ongoing quality assurance and testing activities
- Feedback from users is actively encouraged and used to identify and address usability or accessibility issues as part of continuous service improvement
- Our documentation is available in HTML and PDF formats that meet accessibility guidelines and buyers can request alternative formats if required

2.8 How users work with our service

2.8.1 Browsers

The service is accessible through any modern standards-compliant web browser. As of January 2026, the following browsers are verified as secure and compatible with the platform:

- Google Chrome: Version 144 or higher
- Microsoft Edge: Version 144 or higher (Chromium-based)
- Mozilla Firefox: Version 136 or higher
- Apple Safari: Version 18.3 or higher

2.8.2 Desktop application

Klinik Access does not require a dedicated desktop application. The service is delivered as a browser-based Software as a Service (SaaS) solution and is accessed through supported modern web browsers on desktop and laptop devices.

2.8.3 Mobile

Klinik Access is designed for use on mobile devices through a mobile-responsive web interface. Patients and practice staff can access the service using supported web browsers on smartphones and tablets.

Optimising layouts for touch-based interaction while maintaining access to core functionality, the interface adapts automatically to smaller screen sizes. A dedicated mobile application is not required.

2.8.4 Service interface

Klinik Access provides a secure, role-based service interface for both patients and practice teams.

Patients use a structured digital front door to submit requests for care, provide information, upload images where appropriate and receive messages. Practice staff and clinicians use a professional interface to review and prioritise requests, manage workflows, communicate with patients, collaborate internally and book appointments.

The interface is designed to be intuitive and consistent across devices, with clear navigation, task-based views and dashboards that support efficient day-to-day use. Access to functionality is controlled through role-based permissions.

2.8.5 API

To support integration with agreed NHS and third-party systems, we will provide private APIs. The APIs are used to enable interoperability and data exchange in line with agreed configurations and governance arrangements. APIs are not intended for direct end-user interaction or independent service configuration by buyers.

2.8.6 Accessibility and usability

All interfaces are designed in accordance with WCAG 2.2 AA standards. This includes support for keyboard navigation, screen reader compatibility, readable text, appropriate colour contrast and responsive layouts.

2.8.7 Customisation

To align the service with local operating models, Klinik Access supports configuration-based customisation. Configurable elements include:

- Workflows and routing rules
- Enquiry types and triage pathways
- User roles and permissions
- Messaging content and templates
- Dashboards and reporting views

Customisation is carried out during onboarding by Klinik in collaboration with the buyer. Buyers do not need to undertake custom development. Ongoing configuration changes can be supported through agreed change management processes.

2.8.8 Service levels and availability

The following Service Level Agreements (SLAs) define the availability, responsiveness, and performance standards that apply to the service under the G-Cloud 15 framework:



Metric	Target/standard	Measurement and reporting
Service availability	Minimum 99.99% availability during core operating hours	Continuous monitoring
Planned maintenance	Scheduled outside core hours where possible	Advance notification
Incident response – high severity	Immediate response (within 8 hours at the latest), 24/7	Logged and tracked through service desk
Incident response – medium severity	Response within 1 working day	Service desk reporting
Incident response – low severity	Response within 5 working days	Service desk reporting

Figure 4: Our performance standards

3 G-Cloud alignment information

3.1 Section introduction

This section explains how Klinik Access is onboarded, configured, supported and managed in live operation, from initial service setup through to ongoing support, performance monitoring and secure offboarding at contract end. It sets out the key phases and processes that buyers will follow during the service lifecycle, including onboarding, training, service management and exit arrangements.

Each phase is underpinned by our ISO 27001-accredited management system and supported by defined roles, responsibilities and service levels that align with Crown Commercial Service's G-Cloud 15 framework requirements.

3.2 Onboarding and offboarding processes

3.2.1 Onboarding

Klinik Access is implemented through a structured onboarding and configuration process designed to support consistent, predictable delivery across NHS primary care organisations.

During the initial specification phase, Klinik works with the buyer to agree the custom configuration that is required. This decision is based on the buyer's operating model, service scope and configuration needs. The overall implementation approach is consistent regardless of whether the buyer is new to digital triage or transitioning from a previous supplier.

Implementation from procurement to go-live typically takes:

- Approximately 4 weeks for a standard set-up
- Approximately 4–8 weeks for a custom set-up, depending on the complexity of requirements. We have completed setups within 2 weeks when required

The core implementation steps are as follows:

1. **Specification issued:** We provide a specification template aligned to the agreed service model.
2. **Specification workshop:** Our Customer Success (CS) team holds a structured workshop to confirm workflows, triage pathways, roles and configuration requirements.
3. **Specification agreement:** The final specification is agreed by both parties prior to configuration.
4. **Platform build and configuration:** We configure the platform in line with the agreed specification. No custom software development is required
5. **Training delivery:** We provide role-based training through training videos and, where required, live remote training sessions. The depth and format of training vary depending on whether a standard or custom configuration is selected.
6. **Supplier testing:** We undertake testing to confirm configuration, workflows and access prior to go-live.
7. **Pre-go-live review and supplier sign-off:** We complete a final review to confirm readiness for go-live
8. **Go-live:** The service is made live with remote support in place

The diagram below illustrates a typical onboarding and implementation lifecycle for Klinik Access. The steps shown are indicative and may be adapted to reflect local requirements:

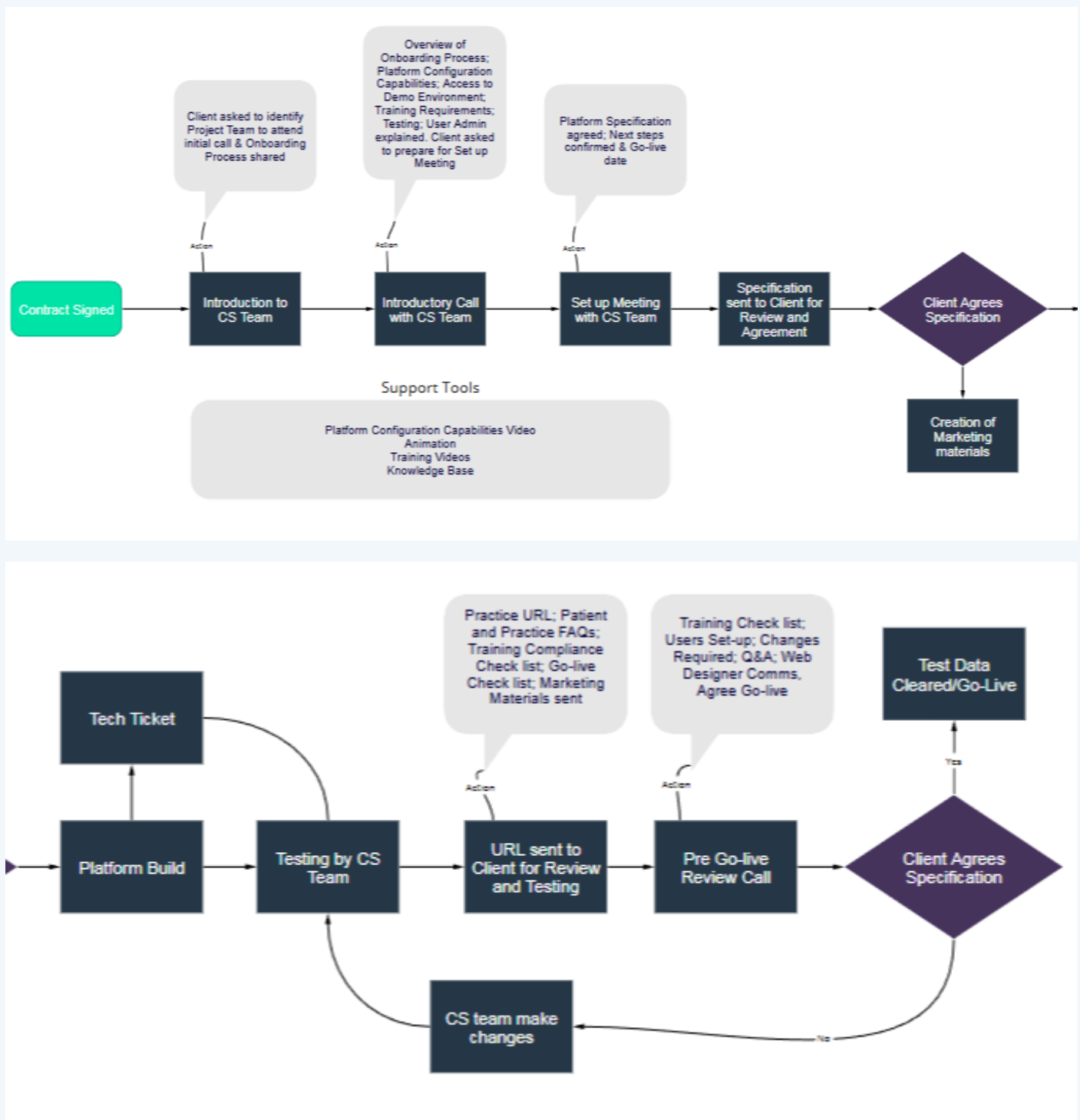


Figure 5: Our onboarding flow chart

3.2.2 Offboarding

To ensure continuity, data protection and clear governance at contract end, we will manage offboarding through a controlled, auditable process that supports data protection obligations. The offboarding process begins with a meeting between Klinik and the buyer to explain the exit approach, confirm responsibilities and agree key dates. To manage and track all offboarding activities, we will then create a dedicated ticket on Jira, our secure issue-tracking and workflow management tool.

As part of this process, we issue the buyer with a contract termination form to confirm and agree the following key milestones:

- The contract end date
- The date the online service will be switched off
- The date by which all patient enquiries have been processed and the data export functionality is enabled

Once the data export feature is enabled, the buyer can download their data using the built-in export functionality. After the buyer has confirmed that all required data has been successfully downloaded, access to the professional interface is isolated by removing all user accounts.

We then raise a further Jira ticket to manage the secure removal of customer data and professional user information from the platform. All associated contact details are also removed from Klinik's customer management systems.

3.3 Data

3.3.1 Data importing and exporting

Ensuring buyers retain control of their data throughout the contract and at contract end, Klinik Access is designed to support straightforward data import and export:

- **Data import:** During onboarding, Klinik supports the setup and configuration of the service based on agreed specifications. Where required, data can be imported to support service configuration and continuity, using agreed formats and secure transfer methods. Data import activities are managed by Klinik as part of the onboarding process to ensure data integrity and security
- **Data export during the contract:** Buyers can export their data at any time using the built-in data export functionality available through the professional interface. Data is provided in open, non-proprietary formats, including CSV, enabling buyers to access and reuse their data without reliance on specialist tools or vendor-specific software
- **Data export at contract end:** At contract end, buyers are provided with sufficient time to export all required data before service access is removed. Data exports include patient enquiries and relevant service data generated during use of the service. Export files are made available in CSV format to support onward use, archiving or migration to another supplier

3.3.2 Analytics

To support performance monitoring and informed decision-making within NHS primary care organisations, Klinik Access includes built-in analytics and reporting capabilities.

The service provides customisable dashboards that present aggregated and real-time data on service usage and demand. This includes visibility of inbound patient enquiries, activity volumes and patterns over time, supporting understanding of workload, capacity and service pressures at practice and network level.

Analytics within the service support day-to-day operational management as well as governance and service review activities. Dashboards are designed to be accessible to authorised users and provide consistent views of demand and activity across practices or networks, where applicable.

Data used for analytics and reporting can be exported in open formats, including CSV, enabling buyers to use the information in external business intelligence or reporting tools if required.

3.3.3 Independence of resource

To ensure that customer performance and availability are not adversely affected by the activity or demand generated by other users of the platform, Klinik Access is delivered as a multi-tenant cloud-based service.

The service is hosted on scalable cloud infrastructure that dynamically manages system resources based on demand. To maintain consistent performance, even during periods of increased usage, we balance workloads across the platform. Logical separation is used to ensure that customer data and configurations are isolated from those of other customers.

System monitoring is in place to track performance, capacity and utilisation across the platform. This allows Klinik to identify and address potential resource contention proactively and ensure that service levels are maintained.

3.3.4 Public sector networks

Klinik Access does not require a direct connection to specialist public sector networks such as PSN, HSCN, JANET, PNN or SWAN to operate.

The service is accessed securely over the public internet using standard HTTPS connections and supported modern web browsers. This allows authorised users to access the service from NHS environments without the need for dedicated network configuration or private network connectivity.

Where required, Klinik Access integrates with NHS systems that are accessed through public sector networks, such as primary care clinical systems and national NHS platforms. These integrations are managed securely and in line with NHS information governance requirements, without requiring buyers to provision or manage direct network connections themselves.

3.3.5 Data-in-transit protection

All data transmitted to and from Klinik Access is protected using industry-standard encryption in transit.

To protect data against interception or unauthorised access while in transit, the service uses secure HTTPS connections with Transport Layer Security (TLS) 1.2 or higher to encrypt data exchanged between user devices, integrated systems and the Klinik Access platform.

To support compliance with NHS information governance requirements and recognised security best practice, we apply encryption consistently across all access routes, including browser-based access and system integrations.

Buyers with enhanced security requirements may use VPN or IPsec connections for additional protection.

3.3.6 Asset protection

Klinik Access is designed to protect customer data and service assets throughout their lifecycle, from storage and processing through to secure deletion and disposal.

- **Data storage location:** All data for UK customers is stored and processed within the United Kingdom on secure ISO 27001-certified cloud infrastructure hosted on Google Cloud Platform. Data residency is maintained in line with NHS information governance requirements
- **Data at rest protection:** Data stored within Klinik Access is encrypted at rest using AES-256 encryption, with encryption keys managed through Google Cloud Platform's Key Management

Service (KMS). Access to stored data is restricted through role-based access controls and is limited to authorised personnel only

- **Datacentre standards:** The service is hosted in professionally managed cloud data centres that meet recognised security and resilience standards. Physical security, environmental controls and redundancy measures are in place to protect infrastructure and maintain service availability
- **Data erasure and sanitisation:** At contract end, and following confirmation that data exports have been completed, customer data is securely deleted from the platform in line with documented offboarding procedures. Data deletion processes are designed to ensure data cannot be recovered once removed
- **Disposal of hardware:** Klinik does not manage physical hardware on customer premises. Disposal of underlying infrastructure hardware is managed by the cloud hosting provider in accordance with recognised industry standards for secure asset disposal and data sanitisation

3.4 Availability and resilience

Klinik Access is designed to remain available and stable for use in live NHS primary care settings, even in the event of infrastructure or system failures. We achieve 99.99% uptime through the following:

- Reducing risk of service disruption, Klinik Access is hosted on resilient UK-based cloud infrastructure with built-in redundancy across core components.
- We continuously monitor service availability and performance. Automated monitoring and alerting enable Klinik to detect issues quickly and initiate investigation and remediation
- Planned maintenance is scheduled outside core UK primary care hours wherever possible and is communicated in advance
- If a service issue occurs, it is managed through a defined incident management process. Incidents are logged, prioritised by severity and escalated appropriately. High-severity incidents are responded to immediately, including outside standard support hours.
- Recovery processes are in place to restore service operation following an incident. These include backup and recovery mechanisms, infrastructure failover and controlled restoration procedures. Where appropriate, we review incidents after resolution to identify root causes and implement preventative improvements

3.5 Governance

Our services are delivered under an Information Security Management System (ISMS) certified to ISO 27001. To oversee compliance and governance, we have a dedicated Governance Team led by Dr Rony Lindell, Medical Director. Supporting this, we have documented policies, procedures and controls covering information security, risk management, incident management and business continuity.

Demonstrating ongoing compliance with NHS information governance requirements, we complete the NHS Data Security and Protection Toolkit annually and hold Cyber Essentials Plus certification.

Service delivery and operational performance is overseen through defined service management processes aligned to recognised good practice, including incident management, change management and problem management.

Security controls and operational processes are subject to regular review and testing, including vulnerability management and independent security assessments.

3.6 Security

3.6.1 Operational security

Klinik Access is operated using defined operational security processes that ensure changes are controlled, vulnerabilities are addressed promptly and incidents are managed effectively.

- **Change control:** All changes to the service are managed through controlled change management processes. Changes are assessed for risk and impact before deployment, tested in non-production environments and released in a controlled manner
- **Vulnerability management and patching:** The service is subject to ongoing vulnerability management. Security updates and patches are applied promptly in line with risk and severity. Dependencies and underlying components are monitored for known vulnerabilities and remediation actions are prioritised to reduce exposure.
- **Continuous monitoring:** Klinik Access is monitored continuously to detect performance issues, security events and anomalous activity. Monitoring and alerting enable rapid identification of potential security or operational issues, allowing timely investigation and response
- **Incident management:** Security and operational incidents are managed through a defined incident management process. Incidents are logged, prioritised by severity and escalated as required. High-severity incidents are responded to immediately, with investigation, containment and remediation actions undertaken. Where appropriate, we complete post-incident reviews to identify root causes and implement preventative improvements

3.6.2 Staff security

Klinik applies proportionate staff security controls appropriate to the nature of the service and the sensitivity of the data processed.

All staff with access to Klinik Access systems or customer data are subject to identity and employment checks prior to being granted access. Screening is aligned to Baseline Personnel Security Standard (BPSS)-equivalent principles, including verification of identity, right to work and employment history.

Access to systems is granted on a role-based and least-privilege basis, ensuring staff can only access the systems and data required for their role. Access is approved through defined processes and reviewed regularly. Access is removed promptly when no longer required, including when staff change roles or leave the organisation.

To ensure security responsibilities are understood and applied consistently across service delivery, staff receive mandatory information security and data protection training as part of onboarding and on an ongoing basis.

3.6.3 Secure development

To reduce risk and protect patient and service data throughout the lifecycle of the service, we develop Klinik Access using secure software development practices.

Security is considered from design through to deployment. Development follows secure coding standards and changes are subject to peer review and quality assurance before release. Development, test and production environments are separated to reduce risk and prevent unauthorised changes.

Automated testing is used to validate functionality and identify defects prior to deployment. Dependencies and third-party components are monitored for known vulnerabilities and are updated where required based on risk and severity.

The service is subject to regular security testing, including independent penetration testing, to validate the effectiveness of technical controls. Findings are reviewed, prioritised and remediated through defined change and risk management processes.

3.6.4 Identity and authentication

To ensure that only authorised users can access the service and that privileged access is appropriately restricted, Klinik Access uses controlled identity and authentication mechanisms:

- All users must authenticate before accessing the service using unique user credentials
- Multi-factor authentication (MFA) is supported to provide an additional layer of security beyond username and password authentication
- User access is managed through role-based access controls, ensuring that individuals can only access functions and data appropriate to their role. Roles and permissions are configured during onboarding and reviewed as part of ongoing service management.
- Privileged access, including administrative and support access, is tightly controlled and limited to authorised personnel only. Additional security controls are applied to privileged accounts, and access is granted on a least-privilege basis.

3.7 Auditing

Klinik Access provides audit logging to support transparency, security monitoring and assurance activities for NHS buyers.

The service records audit logs of user activity within the platform, including access events and key actions performed through the professional interface. These logs support operational oversight, investigation and compliance requirements. Ensuring only authorised users can view audit data, access to user audit information is controlled through role-based permissions.

We also maintain audit logs for supplier activity relating to service operation and support. Where required, audit information relating to supplier actions can be made available to buyers through the support team to support investigation or assurance activities.

Supporting incident investigation, audit and compliance obligations, we retain audit logs and system logs for a minimum of 12 months.

3.7.1 Performance monitoring and metrics

To guarantee service availability and performance, we use automated monitoring and alerting to track platform health, system performance and service availability. Monitoring data is reviewed by the service team to identify incidents, performance degradation or emerging trends that may require intervention.

In addition to technical monitoring, Klinik Access provides operational usage metrics through built-in dashboards available to authorised users. These dashboards present aggregated data on service usage, including volumes of patient enquiries, activity patterns and demand trends. This supports day-to-day operational oversight as well as governance and service review activities at practice, PCN and network level.

3.7.2 Compliance and quality management

The service operates under an ISO 27001-certified Information Security Management System (ISMS), supported by documented policies, procedures and controls covering information security, risk management, incident management and business continuity.

Providing assurance of ongoing compliance with NHS information governance requirements and NHS digital standards, we complete the NHS Data Security and Protection Toolkit annually and hold Cyber Essentials Plus certification.

Service delivery processes are aligned with recognised service management good practice, including defined approaches to incident management, change control and continual improvement. These processes ensure that changes are controlled, issues are addressed systematically and service quality is maintained over time.

Compliance activities, security controls and operational processes are subject to regular internal review. Performance data, service metrics and customer feedback are used to identify improvement opportunities and track corrective actions as part of ongoing service management.

Governance of compliance and quality activities is embedded within Klinik's management structure, with oversight of security, risk and service performance maintained throughout the service lifecycle.

3.8 Backup, restore & disaster recovery

To safeguard all client information, we maintain comprehensive Data Protection, Business Continuity and Information Governance policies aligned with:

- NHS Digital standards
- Data Security and Protection Toolkit (DSPT)
- ISO 22301 Business Continuity Management

Data backup and storage

Data within the Klinik Access system is backed up every 60 minutes. This baseline backup schedule is enhanced through the use of point-in-time recovery (PITR) provided via Google Cloud SQL, allowing restoration to a specific point in time within the recovery window.

All personal data for UK-based practices is stored and processed exclusively in the UK. The service is hosted within the Google Cloud Platform London region (europe-west2), with physical servers located across multi-zone data centres in London.

Recovery objectives

The following recovery objectives apply to Klinik Access:

- **Recovery Point Objective (RPO):** 60 minutes

This reflects the maximum amount of data that could be lost in the event of an incident.

- **Recovery Time Objective (RTO):** 4 hours

This reflects the target timeframe within which the technical support team is able to restore service operation following a major incident.

While we maintain rigorous RPO and RTO targets, these measures remain preventative. Klinik has not encountered a high-severity business continuity incident since launching in 2018. Our multi-zone deployment strategy has successfully mitigated all environmental risks to date without impacting end-user service

Business continuity and resilience measures

Providing assurance that Klinik Access can be restored effectively and within defined timeframes in the unlikely event of a major service disruption, we have a range of business continuity and resilience measures, including:

- **High availability:** To maintain operation in the event of a single-zone outage, the service is deployed across multiple availability zones
- **Geographical redundancy:** Software containers are replicated across multiple geographical locations to protect against catastrophic failures.
- **Real-time monitoring:** The platform is monitored continuously, with automated alerts notifying technical teams immediately when incidents are detected.
- **Continuity planning:** A documented continuity plan is in place to support service migration to an alternative region in the event of a total outage in the primary region.
- **Crisis management:** An annual business continuity exercise is conducted using guidance and templates from the NHS Data Security and Protection Toolkit.
- **Testing and verification:** Restore tests are performed annually, and recovery plans are table-tested with the technical team at least once per year.

3.9 Training

To support effective adoption and use of the service across NHS primary care organisations, we provide training and knowledge transfer as an integral component of every engagement:

- **Training delivery:** We provide training remotely through a series of modular training videos accessed through Klinik's Knowledge Base. The training approach is supported by a learning needs analysis overview, which provides guidance on the most appropriate training pathways for different user types within the practice, such as administrative staff, clinicians and managers
- **Training materials and artefacts:** All training and guidance materials are available through the Knowledge Base accessed through the professional interface. This includes videos, user guidance and functional documentation. Where required, users can download documentation to support learning, reference or local onboarding activities. Accessibility considerations are incorporated into documentation design and content updates
- **Pricing and inclusion:** Training is included as part of the one-off setup and onboarding fee. No additional charges apply for access to standard training materials and guidance provided through the Knowledge Base

3.10 Service pricing

Klinik Access is priced as a Software as a Service (SaaS) offering under the G-Cloud 15 framework (Lot 2b).

The service is provided on a subscription basis, charged per registered patient per year (PPY). Subscription pricing is volume-based, with different price bands applied according to the buyer's total registered patient

population. A one-off setup and onboarding fee applies, which includes configuration and training. Optional add-ons, such as appointment booking functionality, are priced separately where selected.

Full pricing details are published separately in the G-Cloud Pricing Document available on the Digital Marketplace.

3.11 Invoicing process

Klinik Access is invoiced in line with standard public sector procurement and payment practices.

Invoices are issued in accordance with the agreed contract and pricing schedule, typically on a regular billing cycle aligned to the subscription period. Billing arrangements, including whether charges are invoiced monthly in arrears or quarterly in advance, are confirmed at contract award and set out in the call-off contract.

Invoices are issued electronically and reference the agreed purchase order where applicable. Payment terms comply with standard government requirements, with invoices payable within 30 days of receipt.

Accepted payment methods include BACS transfer against a valid purchase order. Any applicable setup or onboarding fees are invoiced separately in line with the agreed implementation milestones.

3.12 Termination terms

Termination of the service is managed in accordance with the terms of the call-off contract agreed under the G-Cloud 15 framework.

The service is subject to a minimum contract term of two (2) years, unless otherwise agreed in the call-off contract.

Following the minimum term, either party may terminate the contract by providing 30 days' written notice, in line with the agreed contractual terms.

Where termination occurs during the minimum contract term, early termination provisions apply. In such cases, a 90-day notice period is required, and any applicable charges or obligations are handled in accordance with the terms set out in the call-off contract.

At the end of the contract term, or where a contract ends early, Klinik follows a controlled offboarding process. This includes agreeing key dates, supporting data export, switching off the service and securely removing customer access and data in line with documented exit procedures.

4 Security and data governance

4.1 Data protection and encryption

All data transmitted to and from Klinik Access is encrypted in transit using Transport Layer Security (TLS) version 1.2 or higher. Secure HTTPS connections are used for browser-based access and system integrations, ensuring that patient data, credentials and service information are protected against interception or unauthorised access while in transit.

The service operates within a secure cloud environment hosted on Google Cloud Platform. Network security controls are used to restrict and protect traffic within the platform, including network segmentation and firewall rules to limit access between system components. Only authorised services and users are permitted to communicate within the environment.

All stored data is encrypted at rest using AES-256 encryption. Encryption keys are managed using Google Cloud Platform Key Management Service (KMS), providing centralised key control, protection and auditability. Access to encryption keys is restricted and monitored in line with defined security controls.

Network activity and system behaviour are monitored continuously to detect anomalous activity or potential security events. Alerts are generated to enable timely investigation and response by the technical team.

4.2 Data at rest, storage locations, and physical security

Klinik Access is hosted on Google Cloud Platform (GCP). All personal data for UK-based customers is stored and processed exclusively in the United Kingdom, within the GCP London region (europe-west2). Data residency is maintained throughout the service lifecycle.

- **Data at rest protection:** All data stored within the service is encrypted at rest using AES-256 encryption, with encryption keys managed via Google Cloud Platform Key Management Service (KMS). Access to stored data is restricted through role-based access controls and monitored in line with defined security processes.
- **Physical security of data centres:** The underlying cloud infrastructure is hosted in multi-zone data centres in London, operated and managed by Google Cloud Platform. Physical security controls at these facilities include layered access controls, 24x7 security monitoring, CCTV surveillance and controlled access to server environments. Physical access to infrastructure is restricted to authorised GCP personnel only.
- **Standards and assurance:** The data centres used by GCP are designed and operated in line with recognised international security standards and are subject to regular independent assurance and audit activities. Klinik relies on these controls as part of its overall security and compliance framework.

4.3 Data sanitisation and disposal

Klinik's data sanitisation procedures align with recognised standards for secure data destruction, including NIST SP 800-88 and DoD 5220.22-M. These standards inform the methods used to ensure data is rendered unrecoverable once deletion has been completed.

All data deletion activities are performed using secure methods provided by Google Cloud Platform (GCP) and are restricted to authorised personnel only.



Data sanitisation process

When a data sanitisation or erasure request is received from a Data Controller, such as a GP practice, Klinik follows a defined process to ensure data is securely removed and cannot be recovered:

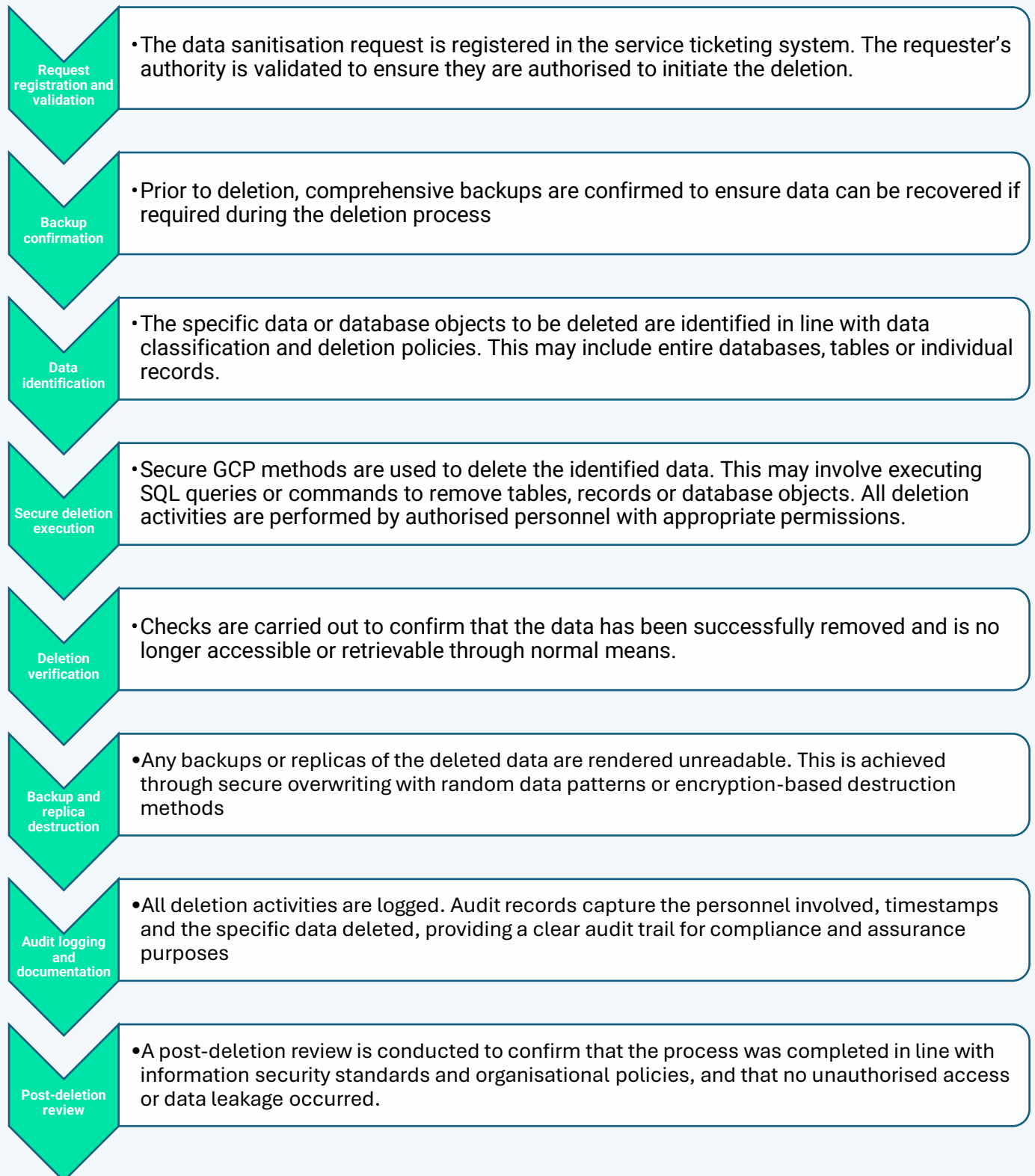


Figure 6: Our data sanitisation process

Hardware and equipment disposal

Klinik does not manage physical hardware on customer premises. Disposal of underlying infrastructure hardware is managed by Google Cloud Platform in accordance with recognised industry standards for secure asset disposal and data sanitisation.

Evidence and assurance

On request, Klinik can provide confirmation that data deletion has been completed in line with the agreed process and applicable standards. All activities are recorded and auditable.

4.4 Security testing and assurance

Klinik Access undergoes regular independent penetration testing, typically on an annual basis, and additionally following significant changes to the platform or its underlying infrastructure.

Penetration testing is carried out by accredited third-party security organisations, including specialist providers such as Silverskin Information Security Oy and Fidus Information Security. These assessments are performed independently of the development and operations teams.

To identify common web application vulnerabilities, testing is conducted in line with recognised frameworks, including the OWASP Top Ten. The scope of assessment includes both unauthenticated and fully authenticated testing of external IP addresses, websites and representative assets within the service.

As part of Cyber Essentials Plus compliance, assessors also perform interactive testing across installed browsers and email platforms. This includes verification that malicious payloads are blocked and that file access requires explicit user interaction.

4.5 Incident and protective monitoring management

To ensure security events are detected promptly, the service is subject to continuous security monitoring, with logs and events collected and analysed to identify potential security incidents, suspicious activity or anomalous behaviour. Monitoring supports detection across application, infrastructure and network layers.

Alerts are generated automatically when predefined thresholds or indicators of compromise are detected, enabling timely investigation by authorised technical personnel. Monitoring operates on a 24/7 basis, ensuring coverage outside standard business hours.

Security events are assessed and classified based on severity and potential impact. A structured escalation process is in place to ensure that incidents are managed by appropriately skilled personnel. High-severity security incidents are escalated immediately, including outside standard support hours, to enable containment, investigation and remediation.

Security incidents are managed through a defined incident response process aligned with ISO 27035 incident management principles. This includes identification, containment, eradication, recovery and post-incident review.

Where a security incident has the potential to impact customer data or service availability, buyers are notified in line with contractual obligations and applicable data protection requirements. Communication is managed through established support and service management channels to ensure clear and timely updates.

4.6 Configuration and change management

All changes to the service are managed through a structured change management process aligned to ITIL change management principles. To ensure that functional, security and operational implications are understood prior to deployment, proposed changes are assessed for risk, impact and dependency before approval.

Changes are categorised by type and severity, with higher-risk changes subject to enhanced review and approval.

All changes are developed and tested in non-production environments before release to live service. For traceability and rollback capability where required, we use version control to manage source code and configuration changes.

Releases are planned and scheduled to minimise disruption to users. Where appropriate, changes are deployed outside core UK primary care operating hours and communicated in advance.

Rollback procedures are in place to enable rapid restoration of a previous stable version should an issue be identified following deployment.

4.7 Information security management and certifications

The service operates within an ISO 27001-certified Information Security Management System (ISMS), supported by documented policies, procedures and controls covering risk management, access control, incident management and business continuity.

Providing assurance of ongoing compliance with NHS information governance standards, Klinik completes the NHS Data Security and Protection Toolkit annually and is certified to Cyber Essentials Plus.

4.8 Secure development and cryptography

To reduce risk and protect data throughout the lifecycle of the service, Klinik Access is developed using secure software development practices, including:

- Controlled access to source code
- Peer review of changes
- Testing prior to deployment

Dependencies and third-party components are monitored for known vulnerabilities and are updated where required based on risk and severity.

To identify and address common web application vulnerabilities, security testing is informed by recognised frameworks, including the OWASP Top Ten. Independent penetration testing further validates the effectiveness of secure development controls.

Cryptographic controls are applied consistently across the service. Data is encrypted in transit using TLS 1.2 or higher and encrypted at rest using AES-256, with encryption keys managed through Google Cloud Platform Key Management Service (KMS). Cryptographic practices are reviewed periodically to ensure alignment with current guidance, including emerging recommendations from the UK National Cyber Security Centre relating to post-quantum cryptography readiness.

4.9 Identity and access management

All users are authenticated before accessing the service. To ensure users can only access functions and data appropriate to their role, we enforce role-based access control (RBAC) is used. Roles and permissions are configured during onboarding and reviewed regularly.

Providing an additional layer of protection beyond username and password authentication, Klinik Access supports multi-factor authentication (MFA), including for administrative and privileged accounts.

The service supports integration with external identity providers where appropriate. This includes support for single sign-on (SSO) using recognised standards such as SAML or OAuth 2.0, including integration with NHS Login for patient access.

5 Supplier information

5.1 About us

Klinik Healthcare Solutions is a healthcare technology company specialising in clinically designed software that improves access to care and patient flow across primary and community healthcare settings.

Founded in 2013 in Helsinki, Finland, Klinik has grown into an established international supplier with operations across the UK, Finland, Portugal and the Netherlands. The organisation combines clinical, technical and operational expertise, with a core team made up of doctors, healthcare professionals and engineers who understand how patient pathways should work in practice.

Klinik focuses on solving one of the most pressing challenges facing healthcare systems today, timely access to care. Patients often struggle to navigate complex systems, while healthcare professionals face increasing demand, administrative burden and inefficient processes. Klinik's solutions are designed to reduce these pressures by enabling:

- Smarter triage
- Better demand management
- More effective use of available resources

Demonstrating the success we have had with our service, we have achieved the following:

We helped a Primary Care Network achieve the following:

- Reduced average waiting times from 4 weeks to 5 days
- 20% reduction in administrative and clinical tasks
- A reduction in DNA rates from 5% to 1%
- Annualised capacity-releasing savings of £340,000

At practice level, customers have reported:

- A 300% increase in the number of patients managed per day
- A 20% reduction in costs through fewer GP sessions required
- A 92% approval rating from healthcare professionals using the service

The company's core products include:

- **Klinik Access**, an AI-driven total triage and patient flow management solution
- **Klinik.AI**, which underpins intelligent routing, prioritisation and decision support

Together, these technologies support accurate history taking, consistent triage decisions and scalable service delivery across GP practices, Primary Care Networks and wider healthcare systems.

Klinik's solutions have supported over 500 healthcare centres and enabled more than 1.5 million patients to access care more effectively. This experience underpins Klinik's approach to delivering secure, clinically led and operationally robust digital services for public sector healthcare organisations.

Klinik's mission is to remove the burden from accessing and delivering healthcare, enabling professionals to focus on patient care while improving outcomes and system efficiency at scale.



>2.5

million
userbase

500

healthcare
centres

5

countries

30

team members

5.2 Relevant experience and testimonials

Klinik Healthcare Solutions has proven track record of delivering digital triage and patient flow management solutions across primary care and wider healthcare settings. Klinik's online triage solutions are currently live in over 300 NHS GP practices in the UK and more than 200 healthcare centres across Finland, Ireland, Portugal and the Netherlands. This experience spans a range of practice sizes and operating models, providing insight into the operational pressures faced by frontline healthcare teams and how digital access solutions can be implemented effectively at scale.

The following case studies demonstrate how Klinik Access has been used in NHS GP practices to improve patient access and reduce pressure on practice teams.

Case study 1 - Portland Medical Centre

Portland Medical Centre introduced Klinik Access in June 2021 to address rapidly increasing patient demand and pressure on GP capacity. Prior to implementation, monthly call volumes had increased by 50% and patients could wait up to 3 weeks for a telephone appointment

Following implementation, Portland Medical Centre transformed how patient requests were managed, achieving the following:

- The practice now processes 100% of patient contacts within 3 days
- Clinicians typically manage 90–100 patients per day without feeling pressured, compared to around 32 patients per day using traditional 10-minute consultations
- Klinik Access enabled the practice to direct patients to the right care first time in 85–90% of cases, compared to 15–20% accuracy using phone-based methods
- The practice reduced monthly phone calls from around 9,000 to fewer than 6,000, freeing capacity for patients who need telephone access
- Staff absence rates reduced from 7% to 3%
- They achieved annual savings of approximately £30,000–£40,000 through more efficient use of resources

Case study 2 - Carn to Coast Health Centres

Carn to Coast Health Centres implemented Klinik Access in 2021 to address rising demand and difficulties prioritising patient need across a large, rural population. The practice serves areas of high deprivation, where physical access to healthcare and digital literacy present additional challenges.

Before implementation, the practice used an online consultation system that made it difficult to assess urgency and prioritise cases efficiently. Clinicians had to search through records to understand patient need, increasing workload and slowing decision-making.

Following implementation, Carn to Coast adopted Klinik as a core demand management tool across online and telephone enquiries. Klinik's AI-driven triage enabled clinicians to identify urgent cases quickly and route patients to the most appropriate professional first time, including pharmacists, nurses, paramedics and mental health practitioners

Within six months of go-live:

- 79% of patients used Klinik online, with 71% accessing the service via mobile
- The practice processed approximately 6,000 patient cases per month
- 78% of patients rated the service as good or excellent

Case study 3 - The Firs Medical Centre

The Firs Medical Centre implemented Klinik Access in 2023 as part of a wider recovery programme following a change in practice management. The priority was to rebuild patient trust, improve access and move from reactive to proactive care delivery

Before implementation, the practice relied heavily on telephone-based access and first-come, first-served appointment allocation. This approach limited the ability to prioritise care based on clinical need and placed significant pressure on reception and clinical teams.

Following implementation, all patient requests now enter a single, consistent triage workflow, regardless of whether patients access the practice online, by phone or in person. As a result:

- GPs manage 90–100 patients per day, compared with around 32 patients per day using traditional 10-minute appointments
- Weekly GP sessions reduced from 31 to an average of 25, releasing clinical capacity
- Overall practice costs reduced by 20%
- Telephone calls into the practice reduced by 20%, easing pressure on reception teams

Testimonials

Demonstrating the positive impact we have had in live primary care environments, we have received the following testimonials from clients:

"We understand our patients like never before. We now have data on the true demand we face in general practice. We have the tools to share the workload across the whole primary care network." **Martin Eades, Managing Partner, Priory Medical Group**



"Now we know what the demand is, we can see the changes that need to be made, and we can manage expectations and optimise the journey for every patient. We can assign the right level of resources to deal with the enquiry, and use the most expensive resource where it is most effective" **Trupti Chauhan,**
Operations Manager, Roxbourne Medical Centre

5.4 How to buy

Klinik's services can be procured directly through the Crown Commercial Service (CCS) G-Cloud 15 Digital Marketplace.

Buyers can search for Klinik on the Digital Marketplace and select the required service listing.

Once selected, the buyer and Klinik will:

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

Ensuring transparency and compliance with public-sector procurement regulations, all engagements are delivered in line with G-Cloud framework conditions. Enabling buyers to adopt the service quickly and compliantly, no further competition or lengthy procurement process is required.

Enquiries or pre-contract discussions can be arranged through our central contact point:

- **Email:** ben.wood@klinik.co.uk
- **Telephone:** 07817287834