

Service Specification

SIMPSi® Assurance

Lot 2b: Software as a Service (SaaS)

1. Service Overview

SIMPSi® Assurance is a robust governance platform that manages processes and assets, such as that within SIMPSi® health, SIMPSi® EHR and SIMPSi® QI, and implementation processes with commissioners, clinicians, NHS managers, commercial partners, and government. Its governance model ensures safety, security, and assurance across clinical, data, operational, and change management.

2. Service Type

Software as a Service (SaaS)

Public cloud deployment

3. Service Features

SIMPSi® Assurance provides the following core features:

1. Trusted digital infrastructure for robust intervention design and delivery
2. Centrally coordinated with role-based access and multi-level authorisation
3. Automated reminders prompting timely actions, reviews, and reporting
4. E-signature approvals for changes, decisions, and releases
5. Mobile-friendly interface managing tasks, approvals, and updates on-the-go
6. Email notifications keeping stakeholders informed and actions on schedule
7. Rule-based workflows enforcing controls and automating agreed decisions
8. Aligned to CE and ISO standards for compliance and security
9. Secure version control with complete change tracking and audit archive
10. Proven at scale, used by hundreds of managers and clinicians

4. Service Benefits

1. Robust governance improving assurance, accountability, and safe decision-making
2. Fully auditable records strengthening transparency, traceability, and compliance
3. Clear accountability lines reducing ambiguity, speeding decisions, supporting safe delivery
4. Escalation management surfacing issues early, routing owners, preventing delays
5. Portfolio oversight tracking delivery, performance, and risk end-to-end
6. Secure-by-design access control reducing information and data risks
7. Embeds standards, controls, evidence trails into everyday workflows
8. Consistent processes and transparent records build control and trust
9. Adapts rapidly to new legislation and emerging evidence
10. Defensible audit trail supporting evaluation, compliance, and legal assurance

5. Service Scope and Constraints

The service is delivered as a fully hosted SaaS solution. The service requires internet connectivity and access via a modern web browser or supported mobile device. Planned maintenance may occur outside core working hours, with advance notification provided. Service availability is dependent on third-party hosting infrastructure. Local configuration may be required to enable integration with organisation-specific systems. Mobile app functionality may vary slightly between operating systems. Offline functionality is limited. Customer IT policies, firewalls or device restrictions may affect access and require local support. Data exchange with external systems is subject to agreed interoperability arrangements.

6. System Requirements

Internet connectivity

Modern web browser (Chrome, Edge, Safari, Firefox)

Organisation firewall allowing HTTPS traffic

Email account for notifications and onboarding

Mobile app requires iOS or Android device

7. User Access and Interface

SIMPSi® Assurance is accessed through a secure, cloud-based web interface. The interface supports role-based workflows for managing governance processes, approvals, and assets. Users can view status, audit trails, and version history through clear dashboards, with all changes safely tracked and archived. The system is centrally managed and designed to support safe, transparent governance across clinical, data, operational, and change management activities.

The mobile app is designed for reviewers only. Admin functionality is managed through a web browser.

The service is designed in line with WCAG 2.2 AA accessibility standards.

8. Customisation

Users can customise elements of the service according to their role. Educational content can be tailored to include locally recorded videos featuring local clinicians or service representatives where available, supporting engagement and recognition.

9. Onboarding and Implementation

We provide a structured onboarding process to ensure users can start using the service quickly and confidently. New organisations receive an initial setup session with a named implementation lead to configure the organisational structure, add local resources and agree rollout plans. Online training is available, including live virtual sessions, recorded tutorials and written guidance. Users also have access to step-by-step documentation and short instructional videos within the platform. We provide launch resources for organisations, including communication templates, local guidance integration and support. Progress review meetings are included to monitor uptake and address any early questions. No technical installation is required. All updates and improvements are delivered centrally, ensuring users always access the latest version without local IT involvement. Optional onsite training can be arranged if required by the buyer.

10. Support

Email and online ticketing support is provided. We reply within 3 working days, but often within 24 hours on weekdays. Phone support is available 9 to 5 (UK time), Monday to Friday.

We provide a single, comprehensive support package included within the annual licence cost. This includes weekday email and online ticket support, with response within three

working days, and priority escalation for service availability issues. Customers also have access to an implementation lead and ongoing contact with our support team. Each organisation is assigned an account manager who acts as the primary point of contact for operational queries, reporting requests and user onboarding. A technical contact is available for integration and access configuration support when required. We provide implementation support during rollout, including virtual onboarding sessions for staff, configuration of organisational structures, and access to training materials. Regular progress review meetings are included in the service and can involve clinical or commissioning leads. System monitoring, maintenance and updates are included at no additional cost. Updates are deployed centrally, ensuring all users benefit from the latest features and security improvements without local installation work. We do not charge extra for standard support. Optional extended support arrangements can be discussed based on local requirements. A cloud infrastructure engineer is available for service continuity and incident resolution.

11. Data Importing and Exporting

Users can export their data through several methods. Organisational administrators can request that data extracts be provided securely in agreed-upon formats upon request. Individual users can view and request to download their own information through the support channels. Where integrations exist, data can also be transferred via agreed interoperability mechanisms.

12. Analytics and Reporting

Service usage metrics are available through commissioner and organisational dashboards. Metrics include number of users, registrations over time, engagement levels, and feature utilisation. Commissioners can monitor population uptake and engagement trends to support service planning and quality improvement. Exportable reports and summaries are available on request, or any metrics required specifically by the organisation.

Reporting types: Through an API, Real-time dashboards, Regular reports, Reports on request

13. Scaling

The service is delivered on a scalable cloud infrastructure with load balancing and automatic resource allocation, ensuring that demand from one organisation does not

impact others. Capacity is monitored continuously and additional resources are provisioned as required. Application and database environments are optimised for multi-tenant use, with logical separation of data and performance safeguards. Traffic management and prioritisation ensure consistent response times. Regular performance testing and system monitoring allow us to maintain service levels and respond proactively to increased demand.

14. Data Protection and Hosting

Data protection between buyer and supplier networks: TLS (Version 1.2 or above)

Data protection within supplier network: TLS (Version 1.2 or above)

Data storage and processing locations: United Kingdom

User control over data storage and processing locations: No

Penetration testing: At least once a year

Penetration testing approach: IT Health Check performed by a CREST-approved service provider

Data sanitisation process: Deleted data can't be directly accessed or Cryptographic Erasure, Data Erasure, Physical Destruction

15. Availability and Resilience

We guarantee a minimum service availability of 99.9% uptime per calendar month for the SIMPSI platform, excluding planned maintenance windows which are notified in advance. The service is hosted on highly available cloud infrastructure with automatic scaling and redundancy to minimise downtime. Availability covers access to patient and clinician applications, authentication services, and core data storage. Planned maintenance is typically performed outside peak usage periods and is designed to have minimal impact on users. Response procedures ensure rapid mitigation and communication. We aim to restore full service as quickly as possible and provide post-incident reporting where required.

The SIMPSI service is designed to be resilient through the use of highly available cloud infrastructure. Patient and clinical data is hosted within AWS, which provides built-in redundancy, load balancing and automatic scaling across multiple availability zones. This ensures continued service operation in the event of underlying hardware or node

failure. Core systems are monitored continuously, with automated failover and rapid recovery mechanisms in place. Regular backups are maintained and replicated to support service restoration. Our deployment approach allows components to be restarted or replaced without user impact. Limited clinician account information hosted within Kinsta's Google Cloud Platform environment benefits from similar underlying resilience and global infrastructure capabilities, with no patient data stored or processed in this environment. We maintain documented incident response and disaster recovery procedures, enabling timely restoration of service following disruption. In the event of a major outage, we work with affected customers to provide updates and ensure continuity of access.

16. Governance and Security

Named board-level person responsible for service security: Yes

Software Security Code of Practice: Yes

Security governance standards: ISO/IEC 27001

We operate a formal Information Security Management System aligned with ISO 27001. Policies cover access control, data protection, secure development, incident management, business continuity, asset management and supplier management. Policies apply to all staff and contractors and are reviewed at least annually or following significant change.

Operational security includes formal configuration and change management, vulnerability management aligned to NCSC guidance, protective monitoring, and incident management based on ISO 27001 and NHS DSP requirements.

User authentication includes Multi-Factor Authentication (MFA), identity federation with an existing provider, and username or password.

Audit information is available on request through the support team. Audit logs and system logs are stored for at least 12 months.

17. Exit and Offboarding

At the end of the contract, users can request the extraction of their data in a structured, machine-readable format. Full data extracts can be provided securely on request in agreed formats such as CSV or JSON, subject to appropriate information governance and security checks. Where integrations are in place, data can also be transferred via

existing agreed interoperability mechanisms. Patient-entered data remains accessible to individual users through their account during the notice period, allowing them to view or download their own information. Once extraction is complete and confirmed by the customer, data will be securely deleted in line with contractual, legal and regulatory requirements, unless retention is required for lawful purposes.

Standard end-of-contract activities are included in the annual licence cost, including data extraction in an agreed structured format, continuation of access during the notice period, and coordinated service closure. No additional cost is charged for standard end-of-contract processes, data export or secure deletion. Optional services, such as bespoke data transformation, migration into third-party systems or extended access beyond the contract end date, can be agreed separately if required by the buyer.