

Service definition — Smart AI Voice Assistant

Supplier: HealthOrbit AI Ltd

Version: 2.0

Date: 29 January 2026

1. What the service is

Smart AI Voice Assistant is a cloud-hosted software service that supports patient access and demand management by capturing requests via voice, structuring key information and routing requests into agreed administrative or clinical workflows. It can support appointment handling and triage workflows as configured by the customer.

Intended users

- Practice teams managing patient access and triage workflows
- Administrators who manage configuration and routing rules
- System administrators responsible for access control and reporting

What the service does

- Captures patient requests via voice interactions where enabled.
- Identifies request type and gathers structured information aligned to customer-defined pathways.
- Supports appointment handling where configured, including booking into available slots.
- Sends reminders or confirmations via configured channels (for example SMS, WhatsApp, or email).
- Routes requests to the appropriate team or queue for review and action.

What the service does not do

- Does not provide emergency services; customers must provide appropriate emergency routing and messaging.
- Does not make autonomous clinical decisions or diagnoses.
- Does not guarantee appointment availability; it supports request capture and routing based on customer configuration.

2. Onboarding and offboarding

Onboarding

- Account setup and role-based access configuration.
- Configuration of pathways, questions and routing rules agreed with the customer.

- Configuration of notification channels where used (for example SMS/email/WhatsApp) subject to customer agreement.
- User onboarding for administrators and operational users.
- Optional pilot/trial setup (including a 14-day trial where agreed).

Offboarding and exit support

- Export of configuration and interaction records in agreed formats, where applicable.
- Support to confirm data extraction and handover (as agreed in the call-off contract).
- Deletion of customer data in line with contractual retention requirements and applicable law.

3. Service constraints and customisation

- Customer policies must define triage, routing and escalation (including out-of-hours handling).
- Configuration is provided through administrative settings; bespoke development is subject to scoping and agreement.
- The service requires a stable internet connection and a supported browser (latest Chrome, Edge or Safari).
- Planned maintenance windows are scheduled and communicated in advance where possible.

4. Service levels and support

Service levels (including availability targets, performance, support hours and incident response times) are agreed in the call-off contract. The service is monitored and incidents are managed through defined triage and escalation processes.

Support

- Support arrangements (hours, response targets, escalation) are agreed in the call-off contract.
- Support channels include email and ticketing; escalation is available for service-impacting issues.

5. Backup, restore and disaster recovery

HealthOrbit maintains backup and recovery processes to support service continuity. Backup frequency, retention, and recovery objectives (RPO/RTO) are defined in the call-off contract, taking into account customer requirements.

- Backups are performed on a scheduled basis and stored securely.
- Recovery procedures are documented and periodically tested.

- Business continuity and disaster recovery plans are maintained and reviewed.

6. Hosting options and locations

The service is hosted on cloud infrastructure. Hosting location (for example UK or EEA region) is agreed with the customer in the call-off contract to meet data residency and information governance requirements.

7. Outage and maintenance management

- Planned maintenance is communicated in advance where possible.
- Unplanned outages are managed through incident response procedures and customer communications.
- Post-incident reviews are conducted for significant incidents and corrective actions tracked.

8. Technical requirements

- Supported browsers: latest versions of Chrome, Microsoft Edge, and Safari.
- Audio/telephony: deployment depends on customer telephony and agreed configuration.
- Optional integration/export: options are agreed in the call-off contract and depend on customer systems.

9. Access to data (upon exit)

- Customer can export relevant outputs and service records in agreed formats.
- Data retention and deletion are managed according to the call-off contract and applicable law.
- A deletion confirmation can be provided on request where contractually required.

10. Security and data protection

HealthOrbit applies technical and organisational measures to protect confidentiality, integrity and availability of customer data. The service supports compliance with UK data protection law, including UK GDPR, through contractual controls and documented processes.

- Role-based access control and least-privilege administration.
- Encryption in transit (TLS) and encryption at rest where applicable to the hosting environment.
- Logging and monitoring to support security event detection and investigation.
- Security incident management procedures, including customer communications and post-incident review for significant incidents.

- Information governance and security documentation available on request (for example policies, DPIA templates, and incident management procedures).

11. After-sales support

- Ongoing customer support and service updates during the contract term.
- Release notes and change communications as updates are deployed.
- Customer check-ins can be provided by agreement to review usage and service performance.