

# Service Definition

## OpenEyes Hosted Application and Support Service

## Table of Contents

|                                                            |           |
|------------------------------------------------------------|-----------|
| <b>1. Service overview</b>                                 | <b>3</b>  |
| <b>2. Service scope – what is included</b>                 | <b>3</b>  |
| <b>3. Backup, restore, and disaster recovery</b>           | <b>5</b>  |
| <b>4. Service exclusions and customer responsibilities</b> | <b>6</b>  |
| <b>5. Service delivery model</b>                           | <b>7</b>  |
| <b>6. Technical requirements</b>                           | <b>8</b>  |
| <b>7. Security, compliance, and assurance</b>              | <b>9</b>  |
| <b>8. Service management and governance</b>                | <b>9</b>  |
| <b>9. Hosting options and locations</b>                    | <b>10</b> |
| <b>10. Pricing model (overview)</b>                        | <b>10</b> |
| <b>11. Term, exit, and portability</b>                     | <b>11</b> |
| <b>12. Service constraints and assumptions</b>             | <b>11</b> |

# 1. Service overview

The OpenEyes Hosted Application and Support Service provides a secure, managed deployment of the OpenEyes ophthalmology electronic patient record (EPR) platform, together with structured application support, system support, and operational assurance services.

The service supports NHS trusts, independent healthcare providers, and international health organisations delivering ophthalmic care. It enables outpatient, surgical, and subspecialty workflows and supports integration with surrounding clinical and administrative systems.

The service may be delivered as a **cloud-hosted Software-as-a-Service (SaaS)** offering operated by the supplier, or as a **client-hosted deployment** where infrastructure is operated by or on behalf of the customer. In both models, service boundaries and responsibilities are clearly defined.

---

## 2. Service scope – what is included

### 2.1 Application hosting

Where delivered as a hosted service, the supplier provides and operates the OpenEyes application stack within a secure cloud environment, including:

- Application runtime environments
- Databases and managed storage
- Secure network configuration
- Backup and recovery services
- High availability configurations appropriate to the selected service tier

Hosting is provided within **UK-based cloud infrastructure by default**, unless otherwise agreed.

Where deployed into client-hosted infrastructure, hosting responsibilities remain with the customer, and the supplier provides support only within the agreed application and system support boundaries.

---

## **2.2 Application support**

Application Support covers operational support for the OpenEyes software as deployed, including:

- Investigation and resolution of application incidents
- Diagnosis of software defects
- Configuration guidance within supported parameters
- Liaison with the OpenEyes open-source governance process for defect resolution

Application Support does not include bespoke development, local code modifications, or prioritisation of new features outside the published governance process.

---

## **2.3 System support**

System Support covers the operation of the underlying platform where this is within the supplier's responsibility, including:

- Infrastructure and service monitoring
- Operating system and platform patching
- Capacity monitoring and routine optimisation
- Backup verification and restore testing

- Cloud service management within agreed scope

Where infrastructure is client-hosted, System Support is limited to advisory support and application-level dependencies unless otherwise agreed.

---

## 2.4 Patch and release management

The service includes deployment of OpenEyes software updates in line with the OpenEyes Lifecycle & Support Standard, including:

- **Long Term Support (LTS) releases**, receiving scheduled maintenance and fixes
- **Current releases**, subject to more frequent updates

Patches are tested and deployed using controlled change processes, with advance notice provided except where urgent security remediation is required.

---

## 2.5 Monitoring and routine maintenance

The service includes continuous monitoring of system health and availability, together with routine maintenance required to maintain security, stability, and performance.

---

# 3. Backup, restore, and disaster recovery

## 3.1 Backup and retention

For supplier-hosted deployments:

- Application data and databases are backed up on a **regular scheduled basis** (typically daily)

- Backups are encrypted and stored securely within the same data residency region
- Backup retention periods are defined according to service tier and regulatory requirements

For client-hosted deployments, backup configuration and operation remain the customer's responsibility unless explicitly included.

---

### **3.2 Restore and recovery**

The service supports restoration of data from backups for operational recovery purposes. Restore procedures are tested periodically to validate recoverability.

Recovery objectives (such as recovery time and recovery point expectations) are aligned to service tier and clinical criticality, and are documented separately where required.

---

### **3.3 Disaster recovery**

Disaster recovery capabilities may include multi-availability-zone or multi-region designs where contracted.

Disaster recovery beyond standard availability configurations is available as an optional service.

---

## **4. Service exclusions and customer responsibilities**

The following are not included unless explicitly agreed:

- Bespoke software development or custom modules
- Support for unsupported or modified third-party extensions

- Responsibility for third-party systems not operated by the supplier
- Local devices, scanners, workstations, or endpoint configuration
- Clinical data ownership, data quality, or clinical governance decisions

Customers are responsible for:

- Appropriate clinical use of the system
  - User access management and role assignment
  - Ensuring endpoint devices meet minimum security and compatibility requirements
  - Contracting separately for third-party systems and integrations
- 

## **5. Service delivery model**

### **5.1 Support hours**

Standard support is provided during UK business hours (Monday to Friday, excluding public holidays). Enhanced and out-of-hours support options are available by separate agreement.

---

### **5.2 Incident management and communications**

Incidents are categorised by severity and impact. For service-affecting incidents:

- Customers are notified through agreed communication channels
- Updates are provided at appropriate intervals

- Escalation routes are clearly defined

Root cause analysis may be provided for significant incidents.

---

### **5.3 Planned maintenance**

Planned maintenance activities are scheduled to minimise clinical disruption.

Advance notice is provided wherever possible, and emergency maintenance is limited to security or stability-critical scenarios.

---

### **5.4 Change management**

Changes are managed through a controlled process including:

- Impact and risk assessment
  - Scheduling and communication
  - Rollback planning where appropriate
- 

## **6. Technical requirements**

The service requires:

- A modern, HTML5-compatible web browser (for example, current versions of Chrome or Edge)
- Secure network connectivity supporting NHS-approved security standards

- Integration with an identity provider (for example Active Directory or equivalent) where required
- Client devices meeting minimum security and performance standards
- Sufficient bandwidth to support clinical image viewing and real-time updates

Additional technical requirements may apply depending on deployment scale and integration scope.

---

## **7. Security, compliance, and assurance**

The service is designed to support NHS and public-sector security requirements, including:

- UK data residency by default
- Alignment with NHS Data Security and Protection Toolkit requirements
- Role-based access control
- Secure authentication and session management
- Audit logging and monitoring
- Incident response and breach management procedures

Security controls are reviewed and maintained in line with recognised industry best practice.

---

## **8. Service management and governance**

The service operates within the OpenEyes open-source governance framework, which includes:

- Controlled release and patch management
- Transparent issue tracking
- Community-led prioritisation of enhancements
- Formal review and approval processes

This approach supports transparency, sustainability, and avoidance of vendor lock-in.

---

## 9. Hosting options and locations

The service supports:

- Supplier-hosted cloud deployments within the UK
- Client-hosted or third-party-hosted deployments by agreement
- Secure private connectivity options (for example VPN or private circuits) where required

Hosting architecture is selected based on scale, resilience requirements, and regulatory considerations.

---

## 10. Pricing model (overview)

Pricing is based on a subscription model reflecting:

- Hosting scale and capacity
- Support tier selected

- Deployment footprint and user numbers

Pricing is published separately within the G-Cloud pricing schedule.

---

## **11. Term, exit, and portability**

The service supports flexible contract terms in line with framework rules.

On exit, customers are supported with:

- Secure export of application data in standard formats
- Delivery of associated artefacts such as documents and audit data where applicable
- Planned transition and knowledge transfer support

Customers retain continued access to the open-source OpenEyes codebase.

---

## **12. Service constraints and assumptions**

The service assumes:

- Operation within supported configurations
- Reasonable and expected clinical usage patterns
- Engagement with published support and governance processes

Significant changes in scale, usage, or scope may require service review.