

iBox Service Definition

1. What the service is

iBox is a software-as-a-service (SaaS) hospital command centre and operational analytics platform. It provides real-time visibility of patient flow, capacity, demand, discharge status, and operational risks across wards, sites, and organisations. The service supports clinical, operational, and managerial users by presenting live data through dashboards, alerts, and standardised operational views to enable timely, informed decision-making.

The service definition document describes how the service operates in practice and is intended to complement, not replace, contractual documents such as product agreements, schedules, and service level agreements agreed with customers.

The service is accessed via a secure, web-based interface and can be used as a standalone platform or integrated with existing hospital systems.

2. Data backup, restore, and disaster recovery

The service is designed for resilience and continuity. Data is stored on resilient, replicated storage and is backed up automatically.

- Backups are encrypted, monitored, and retained in line with documented retention policies.
 - Backup restoration processes are regularly tested.
 - Disaster recovery procedures are documented and maintained.
 - Recovery processes are designed to support restoration of service within agreed recovery time and recovery point objectives.
-

3. Business continuity and disaster recovery

The service operates across resilient cloud infrastructure designed to minimise single points of failure. Capacity automatically scales to manage fluctuations in demand. In the event of a major incident, documented incident and disaster recovery procedures are followed to restore service availability and data integrity.

4. Onboarding and offboarding support

Onboarding

Structured onboarding and implementation support is provided to help organisations start using the service safely and efficiently. This includes:

- Creation of a secure organisation environment
- Configuration of organisational structures, user roles, permissions, and dashboards
- Configuration of integrations where required

- Training delivered remotely or on site depending on organisational needs
- Provision of onboarding materials such as user guides, training resources, and standard operating procedures

Offboarding

On termination of the service, customers can request export of their data in a commonly used, machine-readable format. Data is retained and deleted in line with contractual terms and information governance requirements.

5. Service constraints

- The service is web-based and requires a modern, standards-compliant web browser.
 - Unsupported or end-of-life browsers are not supported.
 - Performance is dependent on customer network connectivity.
 - Buyers cannot directly modify core platform governance, security, or safety controls.
 - Maintenance windows may be scheduled for platform updates, with advance notice provided.
-

6. Service levels

The service is designed to provide high availability and consistent performance.

- Service availability and performance are continuously monitored.
 - Support hours, response times, incident priorities, and resolution targets are defined in the agreed service level agreement (SLA).
 - Incident severity, response times, and resolution targets are applied consistently across customers in line with contractual schedules.
 - Planned maintenance is communicated in advance wherever possible.
-

7. After-sales support

Ongoing support is provided throughout the contract term in accordance with the agreed support schedule and service level agreement. This includes:

- Access to service desk support during defined support hours
 - Incident and problem management aligned to agreed priority levels
 - Configuration and usage support for authorised users
 - Software updates and fixes in line with the product licence
 - Optional additional work or development services subject to agreement and additional fees
-

8. Technical requirements

- Secure internet access using HTTPS
 - Network access allowing HTTPS traffic (port 443)
 - Modern web browser (for example Chrome, Edge, Firefox, or Safari)
 - Compatible with standard NHS desktop and laptop environments
 - No specialist hardware required
-

9. Outage and maintenance management

The service is monitored continuously for availability, performance, and security events.

- Automated alerting is used to identify service issues.
 - Incidents are managed through documented incident response processes.
 - Planned maintenance is scheduled to minimise disruption and communicated in advance.
-

10. Hosting options and locations

The service is hosted in UK-based secure cloud environments. Deployment options may include public cloud, NHS-approved secure cloud platforms, or secure on-premises infrastructure where required and agreed.



11. Access to data upon exit

Upon exit or termination of the service, customers may request export of their organisation's data in a commonly used, machine-readable format, subject to contractual terms.

Data retention, handover, and deletion are managed in accordance with the applicable product agreement, service level agreement, data protection legislation, and information governance requirements. Data is securely deleted following agreed retention periods once contractual obligations have been met.

12. Security

The service is designed to meet recognised security standards and NHS information governance expectations.

- Data is encrypted in transit and at rest
- Role-based access controls are enforced
- Regular security testing is performed, including independent penetration testing
- Changes are managed through formal change control processes
- Security events are monitored and managed through documented procedures

Detailed security, architecture, and assurance documentation is available to buyers on request.