



Service Definition Document

iGROW

Contents

1. Service Overview	3
2. Data Backup, Restore & Disaster Recovery	3
3. Onboarding & Offboarding Support	4
4. Service Constraints	4
5. Service Levels	5
6. After-Sales Support	7
7. Technical Requirements	7
8. Outage & Maintenance Management	9
9. Hosting Options & Locations	9
10. Access to Data (Upon Exit)	9
11. Security	10

1. Service Overview

iGROW is a digital growth chart solution designed to record, monitor, and analyse the growth and development of children and young people. It offers an alternative to traditional paper-based charts with an electronic, data-driven tool integrated into the organisation's EPR or EDMS system.

The system provides clinicians with accurate, up-to-date growth information, supporting clinical decision-making and ensuring consistent monitoring of patient growth trajectories across services. iGROW is typically implemented as a key component of an EPR or EDMS project to support the organisation's transition to fully digital clinical documentation.

2. Data Backup, Restore & Disaster Recovery

The iGROW hosted solution is provided on a HSCN connected service provided by HSO: (<https://www.hso.co.uk>); up to date documents and white papers relating to their service are available on their public website.

Details of the HSO HSCN offering can be found [here](#). The security methodology within HSO can be found [here](#).

HSO has a comprehensive Business Continuity and Disaster Recovery (BCDR) plan in place. Their BCDR plan is designed to ensure the continuity of services and quick recovery in the event of disruptions. Here are the key components included in HSO's BCDR plan:

- **24x7 Support:** HSO provides around-the-clock support to manage and mitigate any issues promptly.
- **Disaster Recovery as a Service (DRaaS):** This service ensures that in the event of a disaster, data and applications can be recovered quickly, minimising downtime and data loss.
- **Data Backup Solutions:** HSO offers robust data backup solutions to ensure that data is regularly backed up and can be restored in case of any data loss incidents. This includes automated backups and secure storage solutions.
- **Business Continuity Planning:** The plan includes detailed steps and protocols to maintain business operations during and after a disaster. This involves risk assessments, impact analyses, and the establishment of recovery objectives to ensure business processes can continue with minimal disruption.
- **Secure Infrastructure:** HSO leverages secure and resilient infrastructure, including co-location services and cloud hosting, to ensure that IT systems remain operational even in adverse conditions. They also provide secure network services to protect against data breaches and other security threats.
- **Regular Testing and Updates:** The BCDR plan is regularly tested and updated to ensure its effectiveness. This includes conducting regular drills, reviewing and updating recovery procedures, and ensuring all staff are trained and aware of their roles during a disaster.

3. Onboarding & Offboarding Support

Onboarding

- Structured implementation methodology covering discovery, configuration, testing, and go-live.
- Dedicated project manager, technical support(s), and account manager.
- Support includes:
 - Service discovery and requirements mapping aligned to local clinical pathways and reporting needs
 - Workflow configuration
 - User role and access configuration for clinicians, administrators, and operational teams
 - User access setup and training
 - Pre-production validation and testing in a non-production environment

Offboarding

- Full extraction of data, including growth records, measurements, audit logs, configuration data, and metadata in open, accessible formats.
- Secure transfer protocols (SFTP, HTTPS, API).
- Decommissioning of service, revocation of access, removal from authentication services, disablement of integrations.
- Data is securely destroyed in line with contractual terms, NHS data handling requirements, and ISO 27001-aligned policies.

4. Service Constraints

Maintenance Windows

- Planned maintenance performed outside business hours where required.
- Advance notice provided for all scheduled downtime.

Customisation

- The platform supports:
 - Configuration based on user access requirements
 - API integration with CRM/ERP systems
- Core system functionality is standardised to maintain system security and stability.

System Access

- Internet connection and modern browser required.
- Access governed by SSO, and role-based access controls.

5. Service Levels

Performance

- Auto-scaling based on live workloads (batch files, on-demand messages, or API requests).

Availability

- 99.9% uptime SLA.
- RTO (Recovery Time Object) is expected to be less than 4 hours using Veeam.
- RPO (Recovery Point Object)
 - Without transaction log shipping – up to 24 hours
 - With transaction log shipping – variable from 5 minutes, to 1 hour

Please note that transaction log shipping involves a higher maintenance fee due to increased offsite storage traffic, and additional storage costs.

Incident Response

Typical response/resolution framework (can be tailored per contract):

Event	Response Time	Communication	Escalation
Incident Detected	Immediate (within 15 min)	Notify teams, begin investigation	Escalate to Disaster Recovery Team if severe
Notify Stakeholders	Within 30 minutes	Inform stakeholders of the incident and next update	Escalate to senior management if severe
Ongoing Updates	Every 30-60 minutes	Update on progress, RPO/RTO expectations	Escalate to vendors if unresolved
Risk of Missing RTO/RPO Targets	After 2 hours	Communicate delay, extended resolution time	Escalate to senior management and technical experts
Post-Recovery Communication	After resolution	Confirm recovery, report downtime and data loss (if any)	Schedule post-incident review

Monitoring

- **Reviews:** Conduct annual reviews and additional reviews as required by the Trust.
- **Review Reports:** Provide detailed review reports outlining findings, changes in risk profile, and proposals for addressing these changes within the cloud service context.
- **Regular Testing:** Conduct regular tests (at least once a year) and additional tests as needed, focusing on cloud service recovery scenarios.
- **Test Reports:** Provide detailed reports on the outcomes of each test, highlighting any failures and proposed remedies.
- **Remedial Measures:** Implement all necessary remedial measures promptly following each test, ensuring the effectiveness of cloud-based disaster recovery.

6. After-Sales Support

Typical after-sales support (can be tailored per contract):

- Dedicated account manager for contract lifecycle.
- Monthly performance reviews.
- Continuous improvement initiatives included as standard.
- Access to technical support team (business hours + emergency out-of-hours).
- Root cause analysis performed for significant incidents.
- Structured escalation route to senior leadership if required.

7. Technical Requirements

Integrations

Import data via:

- HL7 QRY^A19 Search
- HL7 Mata Data consumer

Exported data via:

- HL7 Recipient via MDM^T02
- All data is encrypted using TLS between iGROW and the Trust

We provide an Integration Guide that itemises many of the available integrations that iGROW supports, and more are added every year. There are a number of different kinds of integrations that we support:

- Request parsing
- Authentication & Challenge
- Search & Import

The HL7 Receiving Connector and PDF Export Service are integrations however they are not reusable within other areas of the iGROW architecture or integration pipeline.

Whether the request is passed via a query string (HTTP GET), or a sent as a complete document (HTTP POST), the request parsing integration types takes the input from passed into iGROW and breaks it down into the required components for further processing. Request parsing, if implemented, is always the first integration in the pipeline. In most cases, the resulting component of this integration is a user (either validated on unvalidated) and a patient identifier to be used to populate the patient context. The most common integration we currently supply is the HMAC integration that offers a secure, time limited, tamperproof integration.

The most common search integration we have is the Internal Search used to find a patient in the iGROW database, the next most common is the HL7 Query integration which searches external to iGROW.

User Environment

iGROW has a large family of plugins and components available, as such hospitals are advised to discuss specific needs with Harlow Solutions to tailor the required components to needs. In most cases the standard components of an installation are as follows:

- iGROW Web – the web application that allows users to interact with patient data, and plot and chart measurements
- iGROW HL7 Connector – a metadata receiver that will accept Insert/Update/merge HL7 messages from your PAS/TIE and maintain the patient metadata database
- One or more Single Sign On (SSO) integrations with 3rd party systems that show patients in context Optional or licenced components.

Hosting

iGROW is typically hosted by the Trust/Hospital or by Harlow Solutions on HSCN.

By hosting internally within the Trust, Trusts have full control over the installation, and will need to provide at a minimum the following services:

- Microsoft Windows servers with IIS
- Microsoft SQL Server services
- SSL certificate(s) management for your iGROW installation
- DNS services for the iGROW website names

- HL7 services for any licenced iGROW HL7 components
- AD service account for services/SQL/file share access
- Remote access for installation and support

By hosting with Harlow Solutions on HSCN, Trusts will need to provide the following services:

- Firewall and networking support
- HL7 services for any licenced iGROW HL7 components

8. Outage & Maintenance Management

Planned Maintenance

- Notified in advance with options to reschedule where possible.

Unplanned Outages

- Monitored via system monitoring tools.
- Alerts issued to support teams.
- Incident report provided post-resolution.

9. Hosting Options & Locations

Primary Hosting Locations

- UK data centres.
- Data residency aligned with GDPR, DPA 2018, and Trust requirements.

10. Access to Data (Upon Exit)

All data, including:

- metadata
- audit logs
- archive documents

can be provided in an agreed export format.

Options include:

- Encrypted ZIP archives
- API-based bulk extraction

- SFTP transfers

Deletion of all customer information follows ISO 27001 policies.

11. Security

Certifications & Standards

- ISO 27001 certified
- Cyber Essentials Plus
- NHSE Data Security and Protection Toolkit

Access Controls

- SSO via SAML or OAuth
- Role-Based Access Control (RBAC)
- Full audit logging of user actions

Data Protection

- Data is stored on HSCN Cloud, with HsO – an accredited HSCN supplier, now trading as Syntura (Syntura Group Limited, Registered office: 50 Leaman Street, London, E1 8HQ)
- Data is on UK based servers within HSCN, and is encrypted at rest
- Data storage by internal servers and no third party processing involved
- Penetration testing carried out at regular intervals
- Harlow Solutions have provided a NHSE Data Security and Protection Toolkit
- Access to servers along with the infrastructure are audited by the Trust. iGROW records users and provides an audit trail working in the background: this cannot be viewed by a user; however, we are able to provide the information upon request.
- Segregated production, test, and pre-production environments
- No production data used in non-production systems