

 **Frontier Health****Juno**

**Supportive AI-powered Co-workers
to supplement your workforce**

G-Cloud 15 (RM1557.15) Service Definition

1. Document structure

This Service Definition provides detailed information about the services offered by Frontier under the G-Cloud 15 Framework. It is designed to help public sector buyers understand the functionality, security, pricing and management of Frontier AI's supportive Co-worker service and to provide clarity on how the service is delivered and procured through the framework. The document is structured into three core sections:

1. **Service description:** An overview of the AI Co-workers and Juno offering, including its purpose, core features, benefits, deployment model and user experience, alongside key assurance considerations such as accessibility, security and service scope.
2. **G-Cloud alignment and operational delivery:** Details how the AI Co-workers are delivered, supported and managed under the G-Cloud 15 framework. This section covers onboarding and configuration, service operation, support arrangements, service levels, data management, business continuity, commercial terms and exit processes.
3. **Supplier information:** Provides background information about Frontier, including organisational context, experience and guidance on how buyers can procure the service through the G-Cloud Digital Marketplace.

Each section is designed to allow buyers to quickly locate the information most relevant to their stage in the procurement, contracting or service-delivery lifecycle.

How to use this document

This document supports buyers throughout the full G-Cloud procurement journey, from initial service evaluation through to contract award and ongoing service management.

- For early-stage evaluation, Section 2 (Service description) outlines the scope, capabilities and intended use of the service, helping buyers assess alignment with organisational needs.
- For due diligence and contract preparation, Section 3 (G-Cloud alignment and operational delivery) provides detailed information on onboarding, service management, data handling, support arrangements and exit processes.
- For assurance and compliance, Section 3 also sets out the service's approach to security, resilience, auditing, performance monitoring and business continuity.
- For supplier verification and procurement, Section 4 (Supplier information) summarises Frontier's background and explains how the service can be purchased through the G-Cloud 15 framework.

2. Service description

2.1 About the service

Frontier has developed the 'Frontier AI Co-worker' (Juno), a supportive AI teammate (Co-worker) that compensates for staffing shortages and productivity issues in NHS administrative and clinical teams.

Juno is created using artificial intelligence (AI), business process automation and agentic technology. Juno works alongside existing staff in emergency, in-patient and elective contexts to reduce the burden of daily administrative activities.

The product was designed to enhance administrative efficiency and help mitigate staffing shortages across patient pathways, supporting the delivery of direct patient care. In addition, Juno delivers long-term cost savings by reducing administrative workload, improving pathway efficiency and helping to prevent avoidable delays in patient care.

Delivered under the G-Cloud 15 framework, Juno complements and works on existing clinical and non-clinical systems and is configurable to existing organisational processes.

2.2 Delivery Framework

Designed to support safe, system-agnostic adoption within complex health and care environments, Frontier implements Juno using the following structured delivery framework:



Fast and Accurate: Juno is designed to enable rapid configuration and deployment while maintaining accuracy, consistency and auditability. Juno provides pre-configured workflows, configurability and embedded controls.



Expert: Juno is built to handle the complex, real-world administrative work that NHS teams manage every day. Frontier's team bring significant experience delivering digital programmes across NHS organisations.



System Agnostic: Juno integrates with existing customer infrastructure, working across multiple administrative and clinical systems. Integration is designed to minimise disruption and significant work from customer IT teams.



Safe and Governed: Frontier embeds safety, governance and information assurance into how Juno is configured, accessed and used. The platform supports organisations in meeting clinical safety, data protection and operational governance requirements throughout delivery and ongoing operations.

2.3 Service features and benefits

Juno is designed to support the delivery and management of complex digital health and care services by addressing key operational challenges.

Organisations can adopt Juno's targeted functionality to address specific service pressures or deploy it more broadly to support end-to-end service management. It can also work in non-clinical functions. The platform can be integrated seamlessly with existing clinical and administrative systems, ensuring alignment with operational workflows.

The following features outline the core capabilities of the Juno platform and the benefits it delivers to users, operational teams and organisations:

AI-powered Task Execution

The service automates repetitive administrative tasks across patient pathways using defined rules and workflows, in conjunction with AI. This reduces administrative burden, increases productivity within under-resourced teams and allows staff to focus on higher-value activity. Tasks are handed back to staff as required for human intervention. All tasks are auditable.

Data Quality

Juno interprets information captured across services. This enables teams to reconcile unstructured information more quickly, reducing manual data handling and improving consistency across clinical and administrative records.

Opportunity Identification

Juno proactively identifies opportunities for next steps within patient pathways and supports their execution through automated workflows and targeted task notifications where human oversight or intervention is required. This enables services to improve pathway flow, reduce waiting times and minimise delays caused by manual tracking processes.

Real-time reporting and operational performance dashboards

Juno provides real-time dashboards and reporting on service activity, workload and pathway progress. This improves operational oversight, allowing identification of bottlenecks, monitoring performance and managing risk more effectively.

Secure Role-Based Access Control (RBAC)

Juno enforces secure, role-based access controls aligned to organisational governance and information assurance requirements. This ensures users access only the information and functionality relevant to their role, supporting a safe and secure operation.

System agnostic

Juno supports multiple system integration methods for maximum flexibility and fast deployment.

Conversational AI

Users can talk to Juno to find data or execute tasks on their behalf.

AI-Powered communications

AI-powered communications support service delivery activities. This includes using voice to communicate with staff or patients.

2.4 Service scope

2.4.1 Add-ons and extensions

Juno can be purchased as a stand-alone service.

In addition, it is possible to purchase additional supplementary services such as Juno Enhanced, Premium or Bespoke. It is also possible to purchase discovery packages and additional implementation support.

2.4.2 Cloud deployment model

The Co-worker service is hosted within a secure cloud environment and designed to support scalable, multi-tenant deployment.

To ensure customer data and activity are isolated, Frontier uses logical tenant separation and Role-Based Access Controls. The cloud-based architecture enables rapid deployment, scaling and ongoing service improvements without requiring the buyer to maintain local infrastructure.

Where required, Frontier can adapt deployment and integration approaches to support local governance, interoperability, or information assurance needs, with the details agreed as part of onboarding and documented in the Statement of Work.

2.4.3 Service constraints

There are no service constraints that would prevent public sector buyers from using Juno.

2.4.4 System requirements

To use Juno, buyers require the following minimum system configuration:

- **Supported browsers:** Chrome, Edge or Safari
- **Operating systems:** Windows or macOS
- **Connectivity:** Reliable internet connection for responsive browser access
- **Authentication:** Multi-Factor Authentication (MFA) is enforced

2.5 User support

To ensure buyers can access help quickly, resolve issues efficiently and maintain continuity of operations, Frontier provides a structured and responsive support service for Juno. Frontier's support model aligns with recognised service management best practices and is delivered through a combination of monitored support channels, defined response times and clear escalation routes.

Frontier's support is designed to scale alongside service usage and aims to assure public sector buyers operating in complex, safety-critical environments.

2.5.1 Delivery support details

Buyers can contact the Juno Support Team via email, with telephone support available for emergency incidents.

To ensure visibility, accountability and timely resolution, Frontier logs, tracks and prioritises support requests through a managed ticketing process.

Support availability	- Monday to Friday, 9 am–6 pm (GMT), excluding UK public holidays. - Juno has built-in 24/7/365 monitoring 24/7/365 on-call support for critical issues and incidents
Response times	Support requests are prioritised by severity with the following response targets: - Critical (P0): Response within 2 hours - High priority (P1): Response within 24 hours during working hours - Medium / Low priority (P2/P3): Response within 3 working days
Support request management	All support requests are received via email and managed by a member of Frontier's Support Team. Updates will also be provided via email.

2.5.2 Accessibility and usability

Supporting inclusive adoption by users with a range of accessibility needs, Juno is accessible and usable across public sector environments.

Users access the service through a secure, browser-based interface and do not need to install any local software, however this may change as the service evolves. Users can take advantage of standard operating system and browser accessibility features, including text resizing, zoom, screen magnification and high-contrast settings, where enabled on their device. The interface supports standard keyboard and mouse input and works with built-in assistive technologies available through the user's operating system and browser.

Accessibility considerations are embedded in service design and delivery through usability testing with frontline administrative, clinical and operational users in live NHS environments. This ensures that workflows, task presentation and alerts are clear and usable in day-to-day operations.

Accessibility considerations form part of ongoing service development and improvement. Frontier provides user documentation, onboarding materials and support resources in standard digital formats, including PDF, DOCX and PPTX.

To ensure Juno remains accessible, usable and compliant with public sector expectations, usability and accessibility feedback is continuously reviewed and incorporated to improve subsequent service releases.

2.6 Using Juno

Users access Juno through a secure, browser-based interface that does not require installing local software or applications. This may change as the service evolves.

2.6.1 Interface

Juno provides a clear user interface designed around the day-to-day needs of administrative, clinical and operational users.

Users have real-time visibility of configured workflows, patient information and service performance. The Juno interface presents relevant information clearly, enabling users to review information, monitor progress and take action where required.

Role-Based Access Controls (RBAC) ensure that users have access only to information and functionality appropriate to their responsibilities.

2.6.2 Customisation

Juno is configured to align with local operational context, workflows and governance requirements.

Configuration includes:

- Configuration of workflows to reflect organisational process
- Integrations with existing customer systems

Frontier collaborates with the buyer to configure the service during onboarding and ongoing service operations. This can be selectively taken over by the buyer, as agreed in the SOW.

2.6.3 Service levels and availability

Juno operates across multiple cloud availability zones, with automatic failover in the event of a single-zone failure. Service health and performance are monitored 24/7 using automated monitoring and alerting, supported by on-call engineers.

Service availability commitments and performance targets are agreed upon between Frontier and the buyer during the onboarding process and contractually set out in a contract and Statement of Work.

To support continuous improvement and ensure a consistent user experience, Frontier monitors and reviews service performance is continuously monitored as part of ongoing service management.

3 G-Cloud 15 alignment

3.1 Delivery approach

Frontier delivers Juno through a structured, collaborative delivery model that adapts to each buyer's objectives, scale and governance requirements. The approach combines clear service management controls with the flexibility required to operate safely within complex NHS and public sector environments.

Ensuring accountability throughout the service lifecycle, delivery is underpinned by defined roles, responsibilities and escalation routes. Buyers retain visibility and control at each stage, from onboarding and configuration through to live operation, service review and secure exit. Ensuring consistent quality, transparency and assurance throughout the engagement, this section sets out how Frontier works with buyer teams to deploy, operate and manage Juno under contract.



3.2 Onboarding and offboarding

To ensure buyers can adopt Juno quickly and exit the service securely and transparently when required, Frontier provides structured onboarding and offboarding processes.

3.2.1 Onboarding

Each engagement begins with a structured onboarding process designed to align service configuration, governance and delivery expectations before go-live.

Typical onboarding steps include:

Kick-off and mobilisation	Executive operational and governance stakeholders are engaged to confirm objectives, scope, success criteria, timelines and roles. Governance arrangements, communication routes and escalation pathways are agreed.
Statement of Work (SOW)	A Statement of Work (SoW) is produced setting out service scope, deliverables, dependencies, commercial terms and service management arrangements in line with the G-Cloud 15 contract.
Technical setup and configuration	Technical onboarding in collaboration with the buyer's IT team. This includes configuring the Juno environment, setting up secure access, implementing role-based permissions and where required, integrating with existing clinical or administrative systems.

Workflow and pathway configuration	Juno is configured to reflect local pathways, workflows and operational rules. This ensures the service aligns with existing processes rather than requiring buyers to redesign services around the product.
Testing and readiness	User Acceptance Testing (UAT) is conducted to confirm that workflows operate as expected before go-live.
Training and go-live support	User training and onboarding support are provided before and during deployment, including online training sessions, on-site training (where agreed) and supporting documentation. Go-live is supported to ensure a smooth transition into operational use.

Onboarding is complete once the Juno service is live, users are enabled and the acceptance criteria have been met.

3.2.2 Offboarding

To ensure buyers retain full control of their data and can exit the service without vendor lock-in, Frontier supports secure, transparent offboarding. Typical offboarding steps include:

Offboarding planning and confirmation	Contract end dates, data requirements, retention periods and offboarding timelines are agreed in line with contractual and information governance requirements.
Data extraction and return	Authorised users can export relevant operational and audit data for the applicable retention period. To ensure data is provided securely and in a usable format, Frontier supports data extraction during the offboarding process.
Access review and deactivation	All user accounts are reviewed and deactivated. Administrative access and integrations are deactivated in line with agreed-offboarding procedures.
Data deletion and confirmation	Following successful data extraction, customer data is securely deleted in accordance with data protection legislation, NHS retention requirements and agreed Data Protection Impact Assessments (DPIAs). Confirmation of data deletion is provided
Service closure	The service is formally closed and hand over any remaining service documentation or artefacts as agreed.

Where buyers wish to continue, extend or adapt their use of Juno, this can be agreed through a new or updated Statement of Work (SoW).

3.3 Data

3.3.1 Data importing and exporting

To ensure buyers can bring data into the service easily and recover it at any time without vendor lock-in, Juno supports flexible, standards-based data import and export.

Buyers can export relevant operational and audit data at any time using controlled export functions available to authorised users. To ensure it can be reused or transferred to other platforms, Frontier provides data in open, non-proprietary formats (such as CSV).

At the end of the contract, Frontier supports a structured offboarding process that includes secure data extraction. Ensuring full data portability and a clean exit from the service, buyers can extract their data in line with agreed retention policies and contractual requirements.

3.3.2 Analytics

Juno provides built-in analytics and reporting to support operational oversight, governance and decision-making. Buyers have access to real-time dashboards and reporting covering key service and operational metrics, including:

- Service activity volumes
- Workflow and task status

Buyers can access metrics through the user interface, provided through regular or on-request reports, or other means. Buyers can also export data for use in external reporting or business intelligence tools.

3.3.3 Independence of resource

To ensure that demand from one buyer does not adversely impact the performance or experience of others, Frontier delivers Juno using a multi-tenant cloud architecture.

Frontier separates customer data and activity logically, using tenant isolation and role-based access controls. To maintain consistent performance as demand fluctuates, Frontier continuously monitors capacity and resource utilisation, with scaling mechanisms and alerting in place. These controls ensure reliable service operation regardless of wider platform usage.

3.3.4 Public sector networks

Juno can integrate with approved public-sector networks when required by the buyer.

The service supports connectivity to networks such as the Health and Social Care Network (HSCN), subject to buyer requirements and appropriate governance. Frontier delivers any connection to public sector networks in line with relevant accreditation, security and information governance standards.

Frontier confirms specific network connectivity requirements during onboarding and documents these within the Statement of Work.

3.3.5 Data-in-transit and at rest protection

Ensuring the confidentiality and integrity of data in transit, Frontier protects all data transmitted between the buyer's network and Juno using TLS 1.2 or higher.

Data transmitted within Frontier's network, including communication between internal services and APIs, is also encrypted and protected by strong authentication and access controls.

3.3.6 Asset protection

Juno is hosted within secure cloud environments operated by established cloud providers. The underlying datacentres implement audited physical security controls, including access restrictions, power redundancy, network resilience and environmental safeguards.

Data is encrypted using industry-standard mechanisms. Frontier logically separates customer data within the multi-tenant architecture and restricts access through role-based access controls and least-privilege principles.

To ensure customer data is securely erased at the end of its lifecycle, industry-standard data sanitisation processes are implemented. To prevent recovery, Frontier uses cryptographic erasure or secure deletion techniques.

3.4 Availability and resilience

3.4.1 Guaranteed availability

Juno is designed and operated to deliver high availability using resilient, cloud-hosted infrastructure. Enabling automatic failover in the event of a single-zone failure and reducing the risk of service disruption, the service operates across multiple cloud availability zones.

Frontier monitors service health and performance 24/7/365 using automated monitoring and alerting. An on-call engineering rota is in place to respond to incidents at any time, supported by defined incident management and escalation processes.

If an incident occurs, Frontier:

- Prioritises incidents by severity
- Responds in line with agreed response targets
- Communicates progress and resolution actions to affected buyers
- Investigates root cause and implements corrective actions to prevent recurrence

Resilience is supported by:

- Multi-zone deployment and automated recovery
- Continuous monitoring and capacity management
- Logical tenant separation to ensure one buyer's usage does not affect another

3.5 Governance

To ensure quality, security and continual improvement throughout the service lifecycle, Juno is delivered and operates under a structured governance framework.

Providing buyers with transparency and accountability in how the service is managed day to day, Frontier's governance arrangements define clear roles, responsibilities and escalation routes. To ensure continued alignment with public sector expectations, Frontier regularly reviews service delivery, security and operational controls.

Enabling Frontier to identify improvement opportunities and implement corrective actions where required, Frontier reviews performance data, incident trends and service feedback as part of ongoing service management.

Maintaining accountability at a senior level, named senior roles oversee governance of service delivery and security. This ensures that operational performance, risk management and compliance remain embedded throughout delivery under the G-Cloud framework.

3.6 Security

Frontier embeds security throughout the design, delivery and operation of Juno. To ensure risks are identified, managed and reviewed in line with public sector expectations, Frontier applies a structured security governance framework.

Providing senior accountability and oversight, a named Senior Information Risk Owner has responsibility for service security. They oversee security governance, risk management and compliance activities.

Frontier aligns security practices with recognised industry standards and the UK government's cloud security principles.

To ensure effective assurance, continual improvement and proactive risk management, Frontier regularly reviews security policies, controls and outcomes.

3.6.1 Operational security

Frontier delivers operational security through defined processes that control change, manage vulnerabilities, monitor service activity and respond to incidents.

To ensure that changes are assessed, approved and implemented in a controlled manner to maintain service stability and security, configuration and change management follow a formal change control process.

Vulnerability management combines:

- Regular vulnerability assessment
- Automated scanning
- Monitoring relevant threat intelligence

Frontier has protective monitoring in place to identify suspicious or anomalous activity. Frontier develops Juno following a secure software development lifecycle, embedding security throughout design, build, testing and deployment.

Secure development practices include:

- Secure coding standards
- Code review and quality controls
- Automated testing

- Consideration of security risks during design and change

Ensuring vulnerabilities are identified and addressed promptly, Frontier validates the effectiveness of security controls through regular independent assurance activities, such as penetration testing and security reviews.

3.6.2 Identity and authentication

Access to Juno is restricted to authorised users through strong identity and authentication controls.

User authentication is protected using:

- Enforced multi-factor authentication (MFA)
- Role-Based Access Control (RBAC)

Management and administrative access is restricted to authorised personnel only, requiring elevated permissions and MFA.

3.7 Auditing

To support transparency, governance and investigation of service activity, Juno provides comprehensive audit and logging capabilities.

Enabling buyers to understand how the service is being used and to support compliance, assurance and incident investigation, audit logs capture relevant user actions, system events and administrative activity.

Buyers can access audit information relating to their users' activity through controlled mechanisms, including:

- Access to real-time or near real-time audit information where appropriate
- Provision of audit information on request through the support process

To ensure logs remain available for operational, governance, or investigative purposes, Frontier retains audit data in line with defined retention periods and buyer requirements.

To support transparency and assurance, Frontier can make supplier audit information available to buyers.

3.7.1 Performance monitoring and metrics

To ensure service performance, stability and availability, Juno is continuously monitored, using automated monitoring and alerting to track system health, performance and capacity in real time. This supports early identification of issues, proactive intervention and continuous improvement.

Buyers have access to meaningful usage and performance metrics, including:

- Service activity volumes
- Workflow and task status

Performance data is used as part of ongoing service management to identify trends, support operational decision-making and drive service improvements in collaboration with buyers.

3.7.2 Compliance and quality management

To ensure consistent service delivery and continual improvement, Juno is delivered under a structured quality and compliance framework.

Frontier regularly reviews service delivery, operational performance and security controls as part of ongoing service management. Frontier uses performance data, audit findings and customer feedback to identify improvement actions and track corrective measures.

Governance arrangements define clear accountability for quality, security and compliance activities, while maintaining oversight at the senior management level.

3.8 Backup, restore and disaster recovery

Frontier applies a structured approach to backup, restore and disaster recovery to ensure service continuity, data integrity and rapid recovery in the event of disruption.

Overview and governance

Backups and disaster recovery arrangements are aligned to wider operational resilience and incident management processes. To ensure incidents are managed in a controlled and coordinated manner, recovery procedures define roles, responsibilities and escalation routes.

Resilience is supported by:

- Cloud-hosted infrastructure with built-in redundancy
- Automated monitoring and alerting
- Defined incident and recovery procedures

To ensure they remain effective and aligned with service requirements, Frontier periodically reviews recovery arrangements.

Backup and data protection

Juno uses automated mechanisms to protect data and support recovery, including:

- Automated backups of operational data in line with platform and service requirements
- Encrypted storage of backup data at rest
- Controlled access to backup data, restricted to authorised personnel only

Frontier designs backup processes to ensure that essential operational data and audit information can be restored in the event of data loss or system failure.

Disaster recovery and restoration

In the event of a service disruption, Frontier follows a documented disaster recovery process to restore service availability and data integrity.

Recovery procedures prioritise:

- Restoration of essential service functionality
- Protection of customer data
- Clear communication with affected buyers

Frontier determines response actions and escalation routes based on incident severity.

Frontier coordinates recovery activities through incident management processes, capturing and incorporating lessons learned into service improvement activities.

3.9 Commercial and contractual information

3.9.1 Pricing

Frontier has priced Juno in accordance with the G-Cloud 15 framework, with full pricing details published in the associated Pricing Document.

Pricing is transparent and based on the service configuration selected by the buyer. Any optional features, volume-based pricing or discounts are clearly set out in the Pricing Document.

3.9.2 Invoicing

Invoicing arrangements are governed by the Crown Commercial Service G-Cloud 15 Call-Off Terms and Conditions.

Invoices are issued in accordance with the agreed contract and Statement of Work, with payment terms aligned to standard UK public sector requirements.

3.9.3 Termination terms

Termination of the contract is governed by the Crown Commercial Service G-Cloud 15 Call-Off Terms and Conditions.

Buyers may terminate the contract in accordance with these terms by providing written notice. Frontier may terminate the contract only in circumstances permitted under the Call-Off Terms, such as material breach or non-payment.

Upon termination or contract expiry, buyer data will be handled in accordance with the offboarding and data-deletion processes described in this Service definition.

4 Supplier information

4.1 About Frontier Health

Frontier helps NHS and public sector teams manage increasing workloads and operational pressure by providing supportive AI co-workers that take on routine administrative tasks. This allows staff to stay on top of their work and dedicate more time to the aspects of care that require human judgment. By easing administrative burden and improving workflow, Frontier enables organisations to maintain efficient, reliable services even when resources are stretched.

To strengthen oversight and reduce delays, Frontier provides Juno, an AI co-worker that monitors pathway activity, identifies what needs attention and completes routine actions on behalf of staff. Juno decreases work volume and supports faster, more confident decision-making.

To ensure organisations can adopt supportive AI safely and with confidence, Frontier aligns all solutions with established clinical, operational and governance frameworks. Security, usability and reliability underpin Frontier's approach, enabling teams in regulated environments to gain the benefits of AI without disruption.

Frontier's delivery model is collaborative and outcomes-focused, working alongside client teams to configure and operate Juno in line with local pathways, governance requirements and service priorities.

4.2 Frontier's certifications

Juno is also supported by recognised external assurance and validation. Frontier operates within a robust security and governance framework, including compliance with the NHS Data Security and Protection Toolkit (DSPT).

Providing additional assurance for use within regulated healthcare environments, Juno is registered as an MHRA Class I medical device. Demonstrating our capability, Frontier maintains the following certifications and clearances:

Certifications and Standards	• ISO 27001 Information Security Management Systems • Cyber Essentials Plus • MHRA Medical Device Class 1 (incl. ISO 9001 QMS alignment) • DSPT
Staff clearances	• Background checks conducted at the time of employment • Baseline Personnel Security Standard (BPSS)

4.3 Experience and impact

Juno is successfully deployed in live NHS hospital environments, supporting administrative, operational and clinical teams in performing their everyday work efficiently and safely.

Juno supports high-volume administrative task execution across emergency, urgent and inpatient settings, as well as back-office functions. These deployments demonstrate Juno's ability to operate reliably within safety-critical, regulated healthcare environments while integrating with existing clinical and administrative systems.

Demonstrated outcomes from NHS deployments	Demonstrating Juno's ability to reduce manual workload, improve throughput and support timely patient care, Juno has delivered measurable benefits. For example, in 2025, Juno delivered: • 21.67% reduction in median patient time spent on the pathway • 30% reduction in administrative workforce requirement within hospital departments • Increased productivity as Juno works 24/7, 365 days a year
--	---

Juno's impact and innovation have been externally recognised, including:

Shortlisting for HSJ - Best Contribution to the Improvement of Urgent and Emergency Care (2025/26)	Inclusion as a case study in a World Health Organisation publication, highlighting its contribution to healthcare service improvement
---	--

4.4 User and stakeholder feedback

Demonstrating Juno's suitability for adoption across multidisciplinary NHS teams and its ability to support both frontline delivery and senior operational oversight, feedback from NHS users highlights strong adoption, trust and perceived value:

"This is a game-changer " Divisional Director	"I really love Juno - it is doing a lot of the work for us!" Service Manager
"Juno is more reliable and safer than our current processes." NHS Consultant	"We're so heavily involved in the development of Juno – you're making it work exactly how we want it." Chief Clinical Information Officer

4.5 How to buy

Juno can be procured directly through the Crown Commercial Service (CCS) G-Cloud 15 Digital Marketplace. Once selected, the buyer and Frontier will:

- Agree a Statement of Work (SOW) detailing the service scope, configuration, timescales and pricing
- Enter into a Call-Off Contract under the G-Cloud 15 framework terms
- Issue a Purchase Order (PO) to confirm commencement

Ensuring transparency, compliance and value for money, Frontier delivers all engagements in accordance with the G-Cloud framework conditions. For pre-contract enquiries or clarification, buyers can contact Frontier using the details provided on the Digital Marketplace service listing.