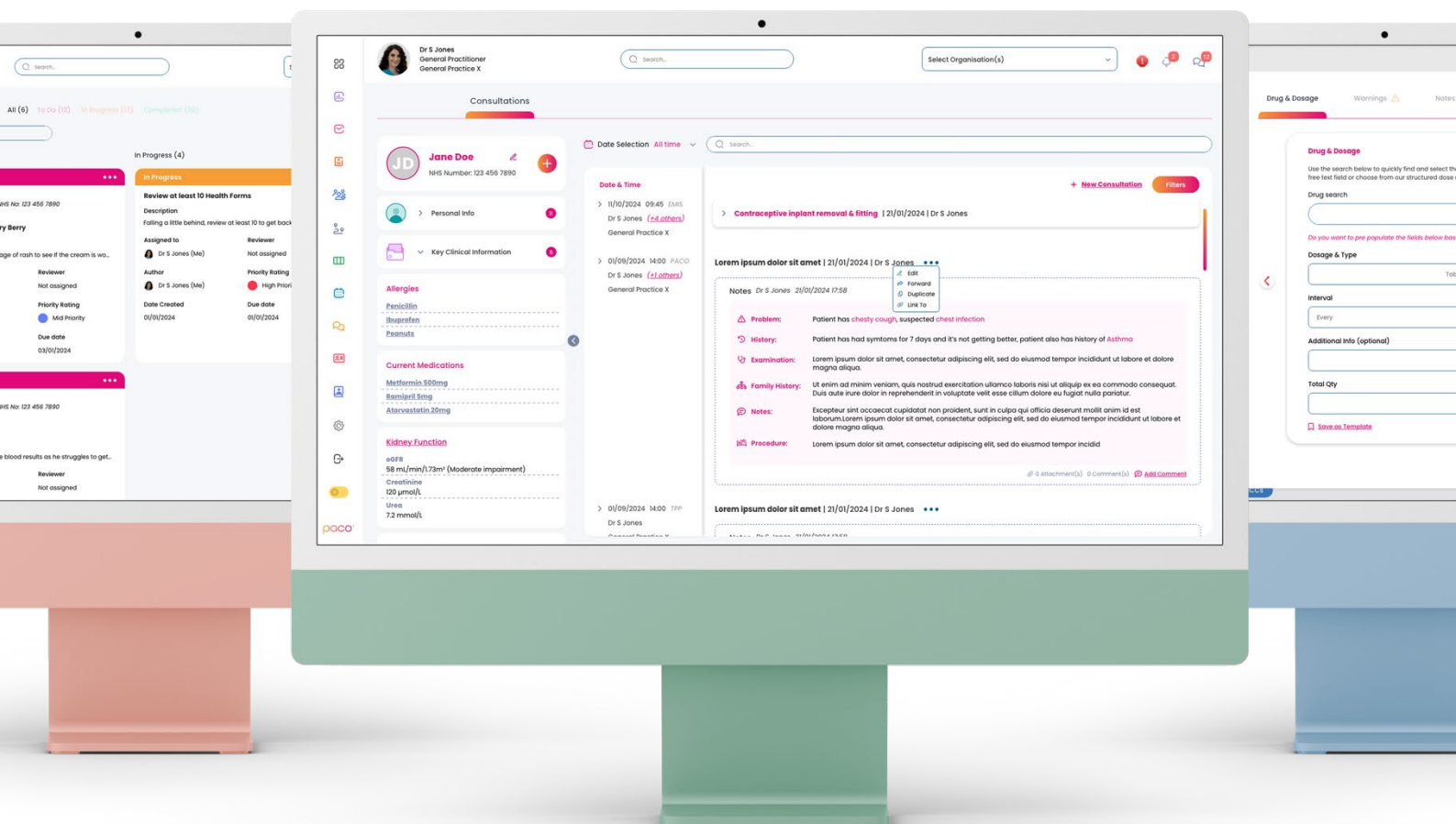


Blinx Patient Portal – Service Definition

PACO – G-Cloud 15



Contents

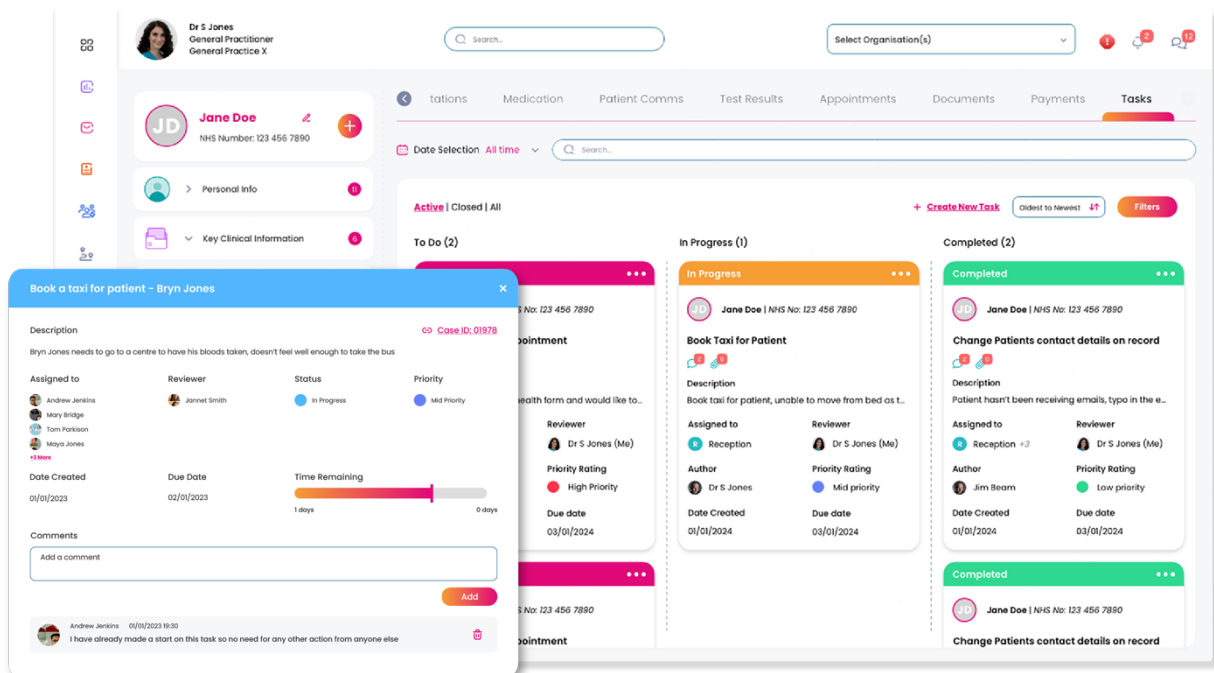
About us.....	3
Blinx Patient Portal	4
Core Capabilities	5
Appointment Management.....	5
Patient Communications	5
Document Sharing.....	5
System Integration.....	5
Security and Governance.....	5
Benefits to Acute Trusts	5
Security and data protection.....	6
Onboarding Support.....	8
Offboarding Support.....	8
Service Constraints.....	8
Service Levels	9
After Sales Support	9
Technical Requirements.....	9
Outage and Maintenance Management.....	9
Hosting Options and Locations.....	10

About us

Blinx Healthcare is a pioneering cloud-based Health Tech company specialising in solutions for Primary Care and Urgent Care settings. Our flagship product suite, PACO (The Patient And Care Optimiser), represents a paradigm shift in healthcare software-as-a-service (SaaS) solutions.

Blinx Healthcare has invested significant time and resources in developing PACO, leveraging advanced technical integration, data analytics, and user experience (UX/UI) expertise. Designed by healthcare practitioners for healthcare practitioners, PACO is built on a modern cloud architecture with scalability at its core.

PACO is the single platform that supports the full patient journey, from GP to hospital and everything in between. PACO brings together GPs, PCNs, Federations, community services, social care, mental health, and hospitals – enabling shared records, real-time communication, and modern digital tools that work with, not against, existing systems.



Blinx Patient Portal

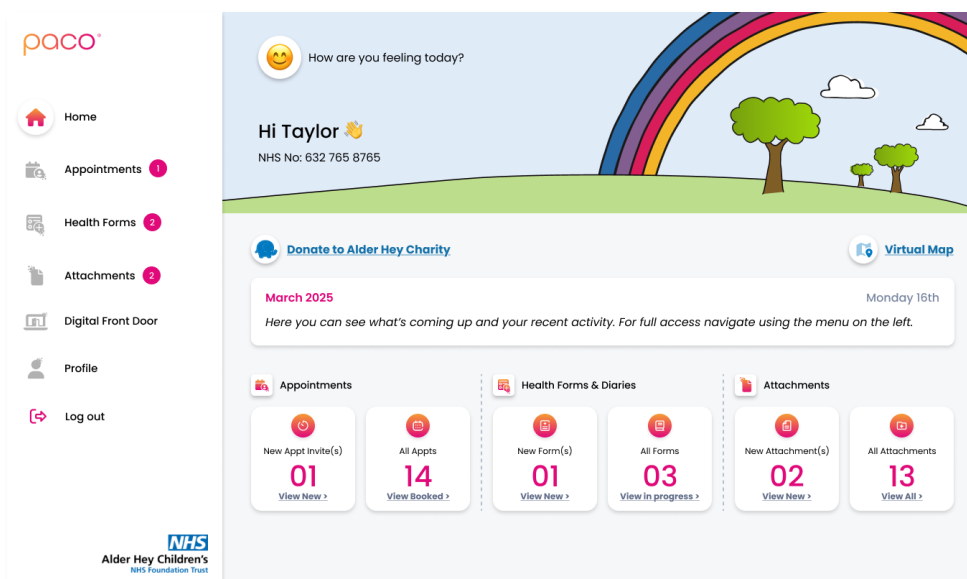
The Blinx Patient Portal is a secure, patient-facing digital access platform designed for **acute Trust environments**. It enables patients to manage appointments, receive communications and access clinical and administrative documents through a single, consistent interface.

The portal integrates with core acute clinical systems (including EPR, PAS and scheduling systems such as Meditech) and can be deployed across outpatient, diagnostic and elective pathways. It is designed to reduce administrative burden, improve patient engagement and support modern access standards at scale.

All data is securely hosted within UK-based cloud infrastructure and aligned to NHS Digital and ISO 27001 standards.

Intended Users

- Acute Trust patients
- Outpatient and booking teams
- Clinical services delivering scheduled care
- Contact centres and access teams
- Trust digital and transformation teams



Core Capabilities

Appointment Management

- Appointment viewing, confirmation and reminders
- Digital attendance confirmation and pre-visit instructions
- Support for high-volume outpatient and diagnostic workflows

Patient Communications

- Two-way digital messaging between Trust and patient
- Automated reminders, updates and pathway messaging
- Reduction in inbound calls and DNAs

Document Sharing

- Secure delivery of letters, clinic outcomes and documents
- Patient access to historical correspondence
- Reduced printing, postage and manual handling

System Integration

- Integration with acute PAS / EPR systems
- Near-real-time synchronisation of appointments and updates
- Configurable workflows aligned to Trust pathways

Security and Governance

- Role-based access controls
- Full audit logging of patient interactions
- Alignment to NHS information governance and DSPT requirements

Benefits to Acute Trusts

- Reduced DNA rates through digital confirmations and reminders
- Lower administrative and contact centre workload
- Improved patient experience and access consistency
- Faster, more reliable communications at scale
- Reduced printing and postage costs
- Better operational visibility of patient engagement

Security and data protection

We prioritise the security, integrity, and availability of user data through robust backup, restore, and disaster recovery measures. Regular backups are conducted with multiple redundant copies stored in diverse UK locations to mitigate data loss risks. With data retention and restore procedures agreed with the IMI supplying systems we comply with the NHS Standards.

We are ISO27001 certified and are DTAC certified with a focus on security of our customers data which is fundamental to our core business, and we have continuous monitoring in place on all our services that is conducting continuous scans of our systems, networks, and applications to identify potential vulnerabilities and security weaknesses.

We have fully documented and monitored Business Continuity plans and processes that meet the NHS Standards and are reviewed every 6 months across the organisation.

Access to Data (Upon Exit)

Users retain ownership and control of their data throughout their engagement with the platform. Upon exiting the platform, users can request access to their data for export or deletion in accordance with data protection regulations, privacy policies, and contractual agreements. Data export tools, data retention policies, and data deletion procedures are provided to facilitate the secure transfer, management, and disposition of user data in compliance with legal and regulatory requirements

Security

We employ a comprehensive set of security measures, protocols, and controls to protect user data, safeguard platform integrity, and mitigate cybersecurity risks and threats. These include but are not limited to:

Encryption

Data transmission and storage are encrypted using industry-standard encryption algorithms (e.g., AES-256) and secure communication protocols (e.g., HTTPS/TLS) to prevent unauthorized access, interception, and tampering.

Access Controls

Role-based access controls (RBAC), multi-factor authentication (MFA), and user authentication and authorization mechanisms are implemented to restrict access to sensitive data, platform features, and administrative functions based on user roles, permissions, and credentials.

Monitoring and Logging

Real-time monitoring, logging, and auditing of user activities, system events, and security incidents are performed to detect, alert, and respond to anomalous behavior, unauthorized access attempts, and suspicious activities in a timely manner.

Vulnerability Management

Regular vulnerability assessments, penetration testing, and security audits are conducted to identify, prioritize, and remediate security vulnerabilities, weaknesses, and exposures across the platform infrastructure, applications, and third-party integrations.

Incident Response

Incident response plans, procedures, and protocols are established and maintained to facilitate the timely detection, containment, investigation, and resolution of security incidents, breaches, and data breaches. Our incident response team is trained, equipped, and empowered to respond effectively to security events and coordinate with internal and external stakeholders, regulatory authorities, and law enforcement agencies as needed.

Compliance and Certification

We adhere to industry-specific compliance standards, regulatory requirements, and best practices to ensure the confidentiality, integrity, and availability of user data, protect user privacy rights, and maintain trust and confidence in our platform and services.

Overall, our security is designed to provide a layered defence approach, comprehensive threat prevention, detection, and response capabilities, and continuous security monitoring, assessment, and improvement to safeguard user data, protect platform assets, and uphold the highest standards of security, compliance, and trustworthiness.

Onboarding Support

Our platform offers comprehensive onboarding support to guide users through the setup process, familiarise them with platform features and functionalities, and maximise user engagement and adoption. This includes personalised face to face training sessions, interactive tutorials, user documentation, and ongoing assistance from our dedicated support team. Below are other onboarding services that can be accessed through the onboarding with new customers

- Custom implementation and service deployment
- Online training and structured business change programme
- Named Account Manager and on-going support through dedicated support management.
- Regular “drop-in” webinar sessions and bespoke clinical and administrative tasks that are focused on PACO features and functions
- Operational support 8am to 7pm Monday - Friday
- Helpdesk available via live chat, telephone and email 8am-8pm, Monday-Sunday (*including Bank Holidays*)
- Out-of hours support for all critical issues identified as Priority 1 incidents
- Customer portal hosting a library of resources, training videos, on-demand webinars, user guides, marketing collateral etc available 24/7

Offboarding Support

Offboarding support services facilitate smooth transitions for departing users, providing data export tools, migration assistance, and knowledge transfer resources to ensure minimal disruption and data continuity.

Service Constraints

Scheduled maintenance windows are coordinated during off-peak hours to minimise user impact, with advance notice provided for planned activities. Customization options are available within predefined parameters to maintain system integrity, security, and compliance with regulatory requirements. Our platform adheres to industry-standard security protocols and best practices to safeguard user data and protect against unauthorised access, breaches, and cyber threats.

Service Levels

Our platform is engineered for optimal performance, reliability, and availability, with guaranteed uptime exceeding 99.9% per our Service Level Agreement (SLA).

Standard support hours are available, with extended support options for critical issues, emergencies, and escalations.

Performance metrics are regularly monitored, tracked, and reported to ensure adherence to SLA commitments and continuous improvement of service quality and user satisfaction.

After Sales Support

Dedicated support is available to address user inquiries, resolve technical issues, and provide guidance on platform usage, configuration, and optimisation. Our support team offers proactive assistance, troubleshooting expertise, and personalised recommendations to enhance user experience, maximise platform value, and drive positive outcomes for individuals and organizations leveraging our services.

Technical Requirements

Users require access to compatible devices (e.g., desktops, laptops, tablets, smartphones) with internet connectivity to access the platform and utilize its features and functionalities. Specific technical requirements may vary based on the services utilized, including operating system compatibility, browser compatibility, and internet connection speed and reliability.

Outage and Maintenance Management

Outages and maintenance activities are communicated to users through email notifications, in-platform alerts, and status updates on our website to keep users informed, manage expectations, and minimize disruption to their workflows and activities. Our service status dashboard provides real-time visibility into platform availability, performance, and maintenance schedules, empowering users to stay informed and plan accordingly.

Hosting Options and Locations

Our platform is hosted on secure, scalable, and resilient infrastructure with redundant data centres located in geographically diverse regions to ensure high availability, fault tolerance, and disaster recovery readiness. Hosting options may include cloud-based hosting solutions, dedicated hosting environments, and hybrid hosting architectures tailored to meet the specific needs, preferences, and regulatory requirements of our users and stakeholders.