HealthForce Connect Service Definition Document

1. What is HealthForce Connect?

HealthForce Connect is a specialist Contingent Workforce Management System which simplifies complex flexible workforce and agency staffing supply chain management, in high-demand frontline healthcare environments.

Healthcare organisations are able to leverage advanced data analytics and automated workflows to enforce Trust / ICB / Framework policies and NHSE Agency Rules to reduce cost, ensure compliance, safeguard continuity and improve quality.

2. Business continuity, data backup and restore, and disaster recovery service levels:

HealthForce Connect ensures robust business continuity, data backup, and disaster recovery service levels to safeguard critical operations and data integrity.

2.1 Business Continuity: HealthForce Connect implements redundancy measures and failover mechanisms to ensure uninterrupted service availability. In the event of hardware failures, network disruptions, or other unforeseen incidents, the platform seamlessly switches to backup systems or alternative infrastructure to maintain continuous operations and minimise downtime. We guarantee a minimum 99% uptime.

2.2 Data Backup and Restore: HealthForce Connect employs automated and regular backups of all critical data to secure repositories. These backups are stored in geographically diverse UK-based locations to mitigate the risk of data loss due to localised incidents. In the event of data corruption, accidental deletion, or other data-related issues, the platform provides robust mechanisms for restoring data from backups quickly and efficiently, ensuring data integrity and availability.

2.3 Disaster Recovery: HealthForce Connect maintains comprehensive disaster recovery plans and procedures to mitigate the impact of major incidents such as natural disasters, cyberattacks, or infrastructure failures. These plans include predefined protocols for assessing the extent of the incident, activating emergency response teams, and orchestrating recovery efforts. Through redundant infrastructure, geographically dispersed UK data centres, and regular disaster recovery drills, the platform ensures rapid restoration of services and minimal disruption to users in the event of a disaster.

By adhering to stringent business continuity, data backup, and disaster recovery service levels, HealthForce Connect provides assurance to users and stakeholders

of its commitment to maintaining operational resilience, preserving data integrity, and safeguarding against potential disruptions or disasters.

3. Onboarding and offboarding support:

3.1 Organisation Setup

During the initial setup and onboarding process, new clients will be led through a comprehensive implementation plan by an assigned team of implementation specialists, supported by our customer success team, to set up their organisation within the platform. This includes tasks such as:

- **3.1.1 Configuring user roles and permissions:** Defining different levels of access and privileges for users based on their roles within the organisation.
- **3.1.2** Customising workflows: Tailoring workflows and processes within the platform to match the client's existing organisational practices and requirements.
- **3.1.3 Integrating with existing systems:** Connecting HealthForce Connect with other software systems or databases used by the client's organisation to ensure seamless data flow and interoperability.
- **3.1.4 Setting up reporting and analytics:** Configuring reporting tools and dashboards within the platform to track key performance indicators (KPIs) and monitor organisational performance.
- **3.1.5 Training administrators:** Providing training and guidance to administrators within the client's organisation who will be responsible for managing and overseeing the use of HealthForce Connect.

3.2 User Onboarding

Our user onboarding process for HealthForce Connect ensures seamless adoption and maximises user proficiency through comprehensive support measures.

- **3.2.1 Platform Demos:** We offer personalised platform demos conducted by our dedicated customer success team. These demos are conducted via video calls with screen sharing, allowing clients to interactively explore the platform's features and functionalities.
- **3.2.2 New User Online Tutorial:** Upon first login, users are greeted with an intuitive new user online tutorial. This tutorial, comprised of interactive wayfinders, guides users through the platform's functionalities step-by-step. It covers essential tasks such as making bookings, utilising AutoAssign, sending direct invitations to preferred healthcare workers, verifying and cancelling bookings, and making multiple bookings in one user session. Users have the option to proceed through the tutorial at their own pace or skip it.

3.2.3 In-App Help Centre: Our platform features an in-app help centre accessible from every page, providing users with instant access to contextualised FAQ and support content. Whether users require assistance with specific features or encounter challenges during their workflow, the help centre offers relevant guidance and resources to address their needs.

Through these comprehensive onboarding and support measures, HealthForce Connect ensures that clients can quickly familiarise themselves with the platform, optimize their utilisation of its features, and receive timely assistance whenever required.

3.3 Offboarding

Our end-of-contract off-boarding process ensures a seamless transition for clients, adhering to contractual terms and data protection regulations while accommodating specific client needs.

3.3.1 Collaboration and Liaison: We collaborate with the client throughout the offboarding process, liaising with any appointed third parties as required / instructed by the client. This ensures clear communication and alignment with the client's expectations and requirements.

3.3.2 Standard Off-boarding: Our standard off-boarding process is simple and straightforward. It involves extracting data from the platform and providing it to the client in an accessible format. Additionally, we secure closure of all client user accounts within an agreed timeframe, in compliance with Call-Off contract terms and Data Protection Laws.

3.3.3 Non-Standard Off-boarding: We support non-standard off-boarding at the client's request, such as facilitating transition to another service provider. This may involve additional steps beyond the standard off-boarding process to ensure a smooth transition.

3.3.4 Resource Uplifts: In the event of a non-standard off-boarding requiring an uplift in resources beyond what is provided during business as usual (BAU), our SFIA rate card will apply. This applies when there is an increase in resource greater than one whole-time equivalent (WTE) provided for more than 5 days prior to the contract termination date, or for more than two days at any time after the contract termination date. However, this is subject to the terms outlined in a mutually agreed off-boarding plan.

By providing clear guidelines and flexibility in our off-boarding process, we ensure that clients can effectively transition out of our services while safeguarding their data and meeting contractual obligations. Our commitment to collaboration and support helps minimise disruptions and facilitates a smooth exit for clients, even in non-standard off-boarding scenarios.

4. Service constraints

HealthForce Connect does not have any constraints. Our updates typically do not require any downtime. It is a lightweight application that doesn't require any additional RAM or computing power.

5. Customisation

HealthFource Connect is fully customisable to individual NHS Trust hierarchies and cost centres, workflows, approval processes, rate cards, policies, compliance requirements, agency supply chain configurations and associated shift cascades, reporting of management information and business intelligence.

6. After Sales Support

6.1 Email and Ticketing Response

- **6.1.1 Non-urgent tickets:** Responses provided within one business day.
- **6.1.2 Urgent tickets:** Responses provided within 4 hours. Users can rank urgency.
- **6.1.3 Triaging:** Questions are triaged through automation and assigned to appropriate support agents.

6.2 Phone Support

24/7 availability for phone support ensures timely assistance for urgent matters.

6.3 Web Chat

- **6.3.1 Availability:** Web chat support available during business hours (9 to 5).
- **6.3.2 Access:** Users initiate conversations via a chat widget on the main website.
- **6.3.3 Real-time Responses:** Users receive responses in real-time within the chat window.
- **6.3.4 Triage and Escalation:** Automation triages questions and routes them to the appropriate support agents. Basic queries are addressed immediately, while complex issues prompt call-backs or further technical support arrangements.

6.4 Online Support

- **6.4.1 Knowledge Bases:** Published knowledge bases assist users in troubleshooting issues independently.
- **6.4.2 Contact Options:** Users can reach the app support team via dedicated email, telephone, or web chat.

6.5 Technical Account Manager and Cloud Support Engineers

6.5.1 **Included in Pricing:** Technical account manager and access to cloud support engineers are included in the pricing model.

6.5.2 **Maintenance and Issue Resolution:** They perform necessary maintenance, issue resolution, or change requests to uphold service quality and ensure a positive user experience.

6.5.3 **Client-Specific Requests:**

6.5.3.1 **Quoting Process:** For client-specific requests beyond the Call-Off Contract, quotes provided using day rates from the SFIA rate card.

6.5.3.2 **Estimated Timeframe:** Estimates given for completion timeframe.

6.6 Support Accessibility Standard

WCAG 2.1 AA or EN 301 549 compliance ensures accessibility for all users, adhering to recognised standards.

This service specification, supported by comprehensive account management, ensures that users receive prompt, accessible, and comprehensive support across various channels, with provisions for both standard and client-specific requests, while maintaining adherence to accessibility standards.

7. Technical requirements

Our service is a lightweight web application designed to meet the following technical requirements:

7.1 Internet Connectivity: The application requires an internet connection to function properly, ensuring seamless access and usability for users across different environments.

7.2 Browser Compatibility: Our application is compatible with most common browsers, including Chrome, Edge, Firefox, Safari, etc. This broad browser support ensures accessibility for users regardless of their preferred browser.

7.3 Mobile Browser Compatibility: In addition to desktop browsers, our application is compatible with mobile browsers, including Chrome, Edge, Safari, and others. Users can access the application conveniently on various mobile devices, ensuring flexibility and convenience.

7.4 Lightweight Architecture: Our application is designed to be lightweight, requiring minimal system resources to operate efficiently. It does not impose significant additional RAM requirements on users' devices, ensuring optimal performance even on devices with limited resources.

These technical requirements ensure our service offers users a seamless and accessible experience, whether they are accessing the application on desktop or mobile devices, and regardless of their choice of web browser.

8. Outage and maintenance management

8.1 Proactive Monitoring:

8.1.1 Continuous monitoring of the service infrastructure to detect potential issues or anomalies.
8.1.2 Real-time alerts and notifications to the operations team for immediate response to any abnormalities.

8.2 Planned Maintenance:

8.2.1 Scheduled maintenance windows communicated to users in advance through appropriate channels (e.g., email notifications, in-app messages).
8.2.2 Maintenance activities conducted during off-peak hours to minimize disruption to users.
8.2.3 Clear communication of maintenance scope, expected duration, and impact on service availability.

8.3 Incident Response:

8.3.1 Rapid response to service outages or incidents to minimize downtime and impact on users.
8.3.2 Incident management protocols followed, including identification, prioritisation, resolution, and communication of incidents.
8.3.3 Regular updates provided to users on the status of incidents and expected resolution times.

8.4 Root Cause Analysis:

8.4.1 Conducting thorough root cause analysis (RCA) for significant incidents to identify underlying causes and prevent recurrence.
8.4.2 Documentation of RCA findings and implementation of corrective actions to address identified issues.

8.5 Change Management:

8.5.1 Formal change management process for implementing changes to the service infrastructure.
8.5.2 Changes assessed for potential impact on service availability, performance, and security.
8.5.3 Changes communicated to users in advance, with appropriate testing and rollback plans in place.

8.6 Service Level Agreements (SLAs):

8.6.1 Defined SLAs for outage response and resolution times, aligned with user expectations and business requirements.

8.6.2 Regular monitoring and reporting on SLA performance to ensure compliance and identify areas for improvement.

8.7 Customer Communication:

8.7.1 Transparent and timely communication with users during outages, maintenance activities, and incident resolution.

8.7.2 Multiple communication channels utilised, including email notifications, in-app messages, and status updates on the service website or portal.

8.8 Continuous Improvement:

8.8.1 Ongoing evaluation of outage and maintenance management processes to identify opportunities for optimisation and enhancement.

8.8.2 Feedback mechanisms in place to gather input from users on their experience during outages and maintenance activities.

By adhering to this service specification, we ensure effective outage and maintenance management, minimising disruptions to users and maintaining high service availability and reliability. Our proactive approach to monitoring, incident response, and continuous improvement enables us to deliver a seamless and resilient service experience for our users.

9. Hosting options and locations

HealthForce Connect is hosted within Microsoft Azure's UK data centre locations to ensure compliance with UK data sovereignty regulations and to meet the specific requirements of healthcare organisations operating within the United Kingdom.

9.1 Cloud Hosting in UK Data Centres:

9.1.1 HealthForce Connect is hosted within Microsoft Azure's UK data centre locations, ensuring that all data residency and sovereignty requirements are met for UK-based healthcare organizations.

Hosting in UK data centers provides assurance to users that their data remains within UK borders, addressing concerns related to data privacy and sovereignty.

9.2 Compliance with UK Regulations:

9.2.1 Hosting HealthForce Connect within Azure's UK data centres ensures compliance with UK data protection regulations, including the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

9.2.2 Healthcare organisations can confidently use HealthForce Connect knowing that their data is stored and processed in accordance with UK regulatory requirements.

9.3 High-Speed Connectivity and Reliability:

9.3.1 Azure's UK data centres are equipped with high-speed network connectivity and redundant infrastructure to ensure fast and reliable access to HealthForce Connect for users located in the UK.

9.3.2 Azure's robust network infrastructure minimises latency and downtime, providing a seamless user experience for healthcare professionals using HealthForce Connect.

9.4 Disaster Recovery and Backup:

9.4.1 HealthForce Connect utilises Azure's disaster recovery and backup solutions within UK data centers to ensure data integrity and availability.

9.4.2 Regular backups of data are performed and stored within UK data centers to mitigate the risk of data loss and ensure compliance with data residency requirements.

9.5 Service Level Agreements (SLAs) for UK Hosting:

9.5.1 Defined SLAs for hosting within Azure's UK data centres guarantee availability, uptime, and performance for HealthForce Connect users.

9.5.2 SLAs are aligned with Azure's service level agreements and tailored to meet the reliability and performance expectations of UK healthcare organisations.

By hosting HealthForce Connect within Microsoft Azure's UK data centre locations, we provide healthcare organisations in the UK with a secure, compliant, and reliable hosting environment. This enables them to effectively manage their workforce and deliver quality patient care while meeting regulatory requirements and safeguarding sensitive health information.

10. Access to data (upon exit)

10.1 Data Retrieval Process:

Upon the termination of a user's access to HealthForce Connect, a defined process is initiated to facilitate the retrieval of their data. The process is designed to ensure

the timely and secure transfer of data to the exiting user or their designated representative.

10.2 Access Request Protocol:

Exiting users or their authorized representatives can submit requests for access to their data through established channels, such as contacting the HealthForce Connect support team or submitting a formal request via email.

10.3 Verification and Authorisation:

Requests for data access are subject to verification and authorization procedures to ensure that only authorised individuals receive access to sensitive information.

Verification may involve confirming the identity of the requester and their relationship to the data being requested.

10.4 Data Delivery Options:

Exiting users have the option to receive their data in a format of their choice, such as a downloadable file or a physical copy.

Secure methods of data delivery, such as encrypted email or secure file transfer protocols, are employed to protect the confidentiality and integrity of the data during transit.

10.5 Compliance with Data Protection Laws:

Data access upon exit is conducted in compliance with applicable data protection laws and regulations, including GDPR and other relevant standards.

Measures are implemented to ensure that the data access process adheres to the principles of data minimisation, purpose limitation, and data security.

10.6 Timeliness and Responsiveness:

We are committed to processing data access requests promptly and responding to inquiries from exiting users in a timely manner.

Clear communication channels are established to keep exiting users informed about the status of their data access requests and any relevant updates.

10.7 Data Retention and Deletion:

Exiting users are informed about the retention period for their data and any applicable data deletion policies. Upon request, we can facilitate the deletion of data in accordance with the user's preferences and legal requirements.

By defining a clear and transparent process for data access upon exit, HealthForce Connect ensures that exiting users can retrieve their data securely and in compliance with data protection laws. This service offering underscores our commitment to data privacy, transparency, and customer satisfaction.

11. Security

11.1 Named Board-level Person Responsible for Service Security:

A designated board-level individual is accountable for overseeing service security, ensuring clear ownership and accountability at the highest level.

11.2 Security Governance:

Security governance is certified, adhering to ISO/IEC 27001 standards, indicating a structured and compliant approach to security management.

11.3 Information Security Policies and Processes:

Our Cyber Security Management Framework aligns with ISO 27001 and NCSC's GDPR Security Outcomes, approved by the Board. Supporting policies and technical standards prescribe security objectives, with responsibility matrices in place for maintenance. An IT user policy ensures staff adherence, with controls regularly tested, assessed, and audited, with outcomes reported to the business.

11.4 Operational Security:

Supplier-defined controls ensure robust management of configuration and changes, with continuous tracking of service components and a CI/CD strategy.

11.5 Vulnerability Management:

Supplier-defined controls govern vulnerability management, with a comprehensive approach to vulnerability assessment across all environments.

Severity-based prioritization determines the application of fixes, with critical vulnerabilities addressed promptly, especially those actively exploited in the wild.

11.6 Protective Monitoring:

Security event logs are generated from all system components, monitored by a UK-based SOC team utilising advanced SIEM solutions.

Events are categorised based on severity, with response timelines determined accordingly to mitigate potential compromises effectively.

11.7 Incident Management:

Conforming to recognised standards such as CSA CCM v3.0 or ISO/IEC 27035:2011, incident management follows structured playbooks for response activities. Customers can report suspected incidents to the application support team, with incident reports provided to impacted parties through the customer relationship function.

11.8 Staff Security:

Staff undergo screening procedures, though not conforming to BS7858:2019, ensuring a baseline level of personnel security clearance up to BPSS standards.

11.9 Secure Development:

Adherence to secure software development best practices includes independent review of processes, ensuring compliance with industry standards such as CESG CPA Build Standard, ISO/IEC 27034, ISO/IEC 27001, or CSA CCM v3.0.

This service definition ensures a robust and comprehensive approach to security management, encompassing governance, policies, operational practices, vulnerability management, monitoring, incident response, staff security, and secure software development.