G-Cloud 15
Service Definition Document
Graphnet Shared Care Record

Author: Graphnet Health Limited

Version: 1.0

Created: 30 January 2026

Confidentiality / Document control

The materials contained in this document contain Confidential Information and Trade Secrets of Graphnet Health Limited including, but not limited to: proprietary formulas; marketing and advertising methods; pricing information; financial information; ideas; concepts; processes and other information relating to the business of Graphnet Health Limited.

Confidential information may also include material non-public information that may not be further disclosed or used except in strict compliance with this confidentiality provision and all relevant UK, EU and/or other applicable national commercial, confidentiality or securities laws.

Recipient of this document shall maintain the confidentiality of the Confidential Information and Trade Secrets contained herein and shall not release, publish, reveal or disclose, directly or indirectly, such Confidential Information or Trade Secrets to any other person or entity without first obtaining the prior written consent of Graphnet Health Limited.

By retention of this and related documents, any recipient covenants that the Confidential Information and Trade Secrets shall only be used for the purposes intended hereby and shall not be exploited in any other manner. Any Recipient shall not make, or permit to be made, except in furtherance of the express purposes intended hereby, any copies, abstracts, or summaries of the material contained in this and related documents.

Graphnet Health Limited retains title to this document, and, upon termination of the business arrangement discussed hereby, Recipient covenants that it shall promptly return or destroy this document and all documents associated therewith, whether prepared by the Recipient or Graphnet Health Limited, retaining only one copy of such documents as may be necessary to document its decision with respect to proposed business arrangement.

Table of contents

1 Graphnet Introduction

Graphnet Health was formed over 25 years ago and is today the UK's no.1 leading supplier of:

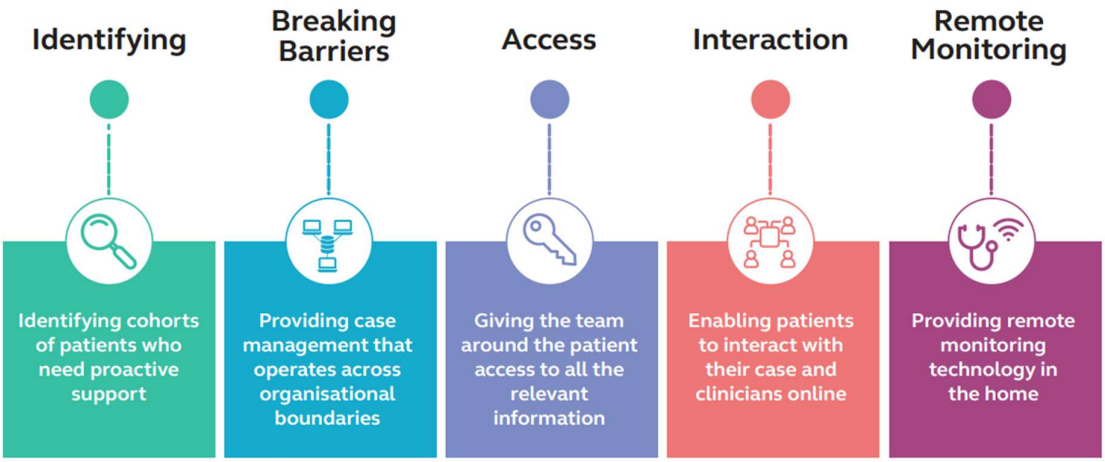
Shared care record (SCR) software and services

Population health analytics (PH)

Remote monitoring solutions (RM)

Graphnet provides shared care records and population health solutions across entire care communities, holding health and care information on over 20m patients. Our solutions are designed to support the delivery of integrated care services by providing access to a single, secure electronic patient record.

It combines a shared record with community-wide assessment, workflow, care planning, and specialist apps for long-term conditions. It also supports patient engagement, through the use of the myGraphnet Personal Health Record, and population health management. Graphnet's integrated record software is used by 11 ICBs and covers approximately one third of the population in England.



Our health and social care solutions allow for the integration of services across whole care communities for better, safer care. This is achieved by linking information from multiple systems, integrating workflows between care settings, supporting multi-provider reporting &

analysis and engaging patients to self-care.

Our solutions use leading edge technologies - including mobile, wearables, instant messaging, the cloud and machine learning - to radically improve services and the way care professionals and patients interact together.

The 10 Year Health Plan for England outlines three significant shifts aimed at transforming the NHS:

- Hospital to Community: Reducing reliance on hospitals and focusing on community health services.
- Analogue to Digital: Transitioning to digital technologies for better healthcare delivery.
- Sickness to Prevention: Prioritizing prevention over just treating illness to improve overall health outcomes.

These shifts are designed to enhance the efficiency and effectiveness of the NHS, aiming to improve patient care and reduce waiting times.

Graphnet's solutions align with the NHS 10 Year Plan by supporting improved outcomes, earlier interventions, and more efficient use of services. Our SCR combined with Population Health and Care Coordination platforms, is designed to support Integrated Care System (ICS) development, reduce pressure on urgent and emergency care, support a move to more proactive, preventative, population health-based models of care, and empower patients. This supports the initiative to move more care into the neighbourhood.

Our solution helps systems identify at-risk cohorts and act using near real-time information from both primary and secondary care, enabling local multi-disciplinary teams to proactively manage care and reduce non-elective demand.

Care coordination tools facilitate team-based interventions through task management, assessments, shared plans, and alerts. This approach underpins key NHS priorities such as age-friendly care, long-term condition management, and reducing health inequalities, thereby

delivering on the NHS Long Term Plan's goals.

Our ethos is to work closely and collaboratively with our customers and IT partners. Our mission is to make a lasting difference to care outcomes by supporting the delivery of modern, integrated NHS and local authority care services.

2 An overview of Graphnet Shared Care Record G-Cloud Service

The Graphnet Shared Care Record is the UK's most widely used electronic health and shared care record; it is a Single Patient Record. It stores and **shares data for approximately 20m individuals** from all health and social care settings including primary, acute, mental health, community, social care, out of hours, ambulance and other specialist settings. Our SCR comprises of the following core and optional modules:

Data Repository: This creates an enterprise master patient index and matches, stores and organises a wide range of data from all care settings.

Clinical Portal: A web-based portal which provides a unified view of data from multiple source systems, integrated into a single, shared care record at the point of care, a Single Patient Record. The portal is intuitive to navigate and uses clear and consistent screens to present relevant data to users. It also includes a wide range of IG and functional features including Role Based Access Controls (RBAC), views configurable by user type and care setting, and full audits of user activity.

As well as supporting standalone web access, the portal can be embedded into local applications using Single Sign On (SSO) and patient context searching so that users can view the shared record for a patient from their local clinical system, without having to log in or reselect the patient.

The SCR also allows secure, integrated access to third party systems to allow users to view information held in external record services such as GP Connect, and the National Care Record Service.

Highway: Our solution's integration engine, which uses the Rhapsody platform, and is pre-configured to collect a rich data set from many systems used by English health and social care providers. We have connections to over 100 different provider solutions including all the key systems in use across England such as **EMIS Web (Optum), TPP SystmOne, Docman,**

Medway/CareFlow EPR, Care Director, CarePlus CHIS, Cerner Millennium, EPIC, Allscripts, Liquidlogic, Access Mosaic, RIO and many more. Data is loaded at various frequencies ranging from real-time to daily depending on the functionality of the source systems.

Care Plans: A growing number of different care plans are available for use in our shared record, allowing users to contribute to shared care planning across a community, rather than multiple copies being maintained across several local systems. Specific care modules are available for End of Life, Respect, Comprehensive Geriatric Assessments (CGA), Heart Failure, Frailty, Learning Disability & Autism, Diabetes, Dementia, Pregnancy Monitoring, and other areas. The About Me care plan, which can be contributed to by the clinical teams and the patient alike and is accredited to the national PRSB standard, and the digital Respect plan has been accredited and endorsed by the National Resuscitation Council for display both in the shared record and through the patient application view. Our CGA care plan is the first to be digitalised in the NHS.

MyGraphnet Personal Health Record: Provides patients and citizens with secure access to their shared care record via their NHS Login account; the ability to record and contribute information; participate in their care, access relevant health and wellbeing information and find out about care services. Data contributed by individuals is made available to clinical users through the clinical portal.

MyGraphnet Care Apps: Specialist applications supporting patients to participate in their care and manage specific conditions allow the individual to record specific observations such as monitoring of oxygen saturations, blood pressure, blood sugar and/or to record important factors about themselves to share with their care teams.

These application modules also allow the care teams to share treatment plans, advice and information with patients. Other care applications include intensive cancer treatment support, COPD, heart failure and epilepsy.

Graphnet Remote Monitoring (powered by Luscii): In addition to the myGraphnet Care applications, our Remote Monitoring suite of products, powered by Luscii, is part of the Graphnet offering. This includes an integrated solution for the management of patients with

long-term conditions or episodic health events in the home, or other locations remote from their centre of care. The platform supports wider device integration, video consultations, and includes the option of dedicated tablets for patients who may not be able to use their own smartphones or tablets. Further details are available under a separate service line.

Graphnet Population Health: We use the Microsoft Azure cloud-hosted analytics platform to ensure that the full breadth of shared care record data (plus national and local data sources) is available to support direct care, secondary uses (pseudo-anonymised) and research (anonymised). Our solution Includes **tightly coupled integration** of analytics content into the clinical portal at both patient and cohort level.

2.1 The Graphnet Shared Care Record and Population Health working together : cohort identification (Case Finding) and management

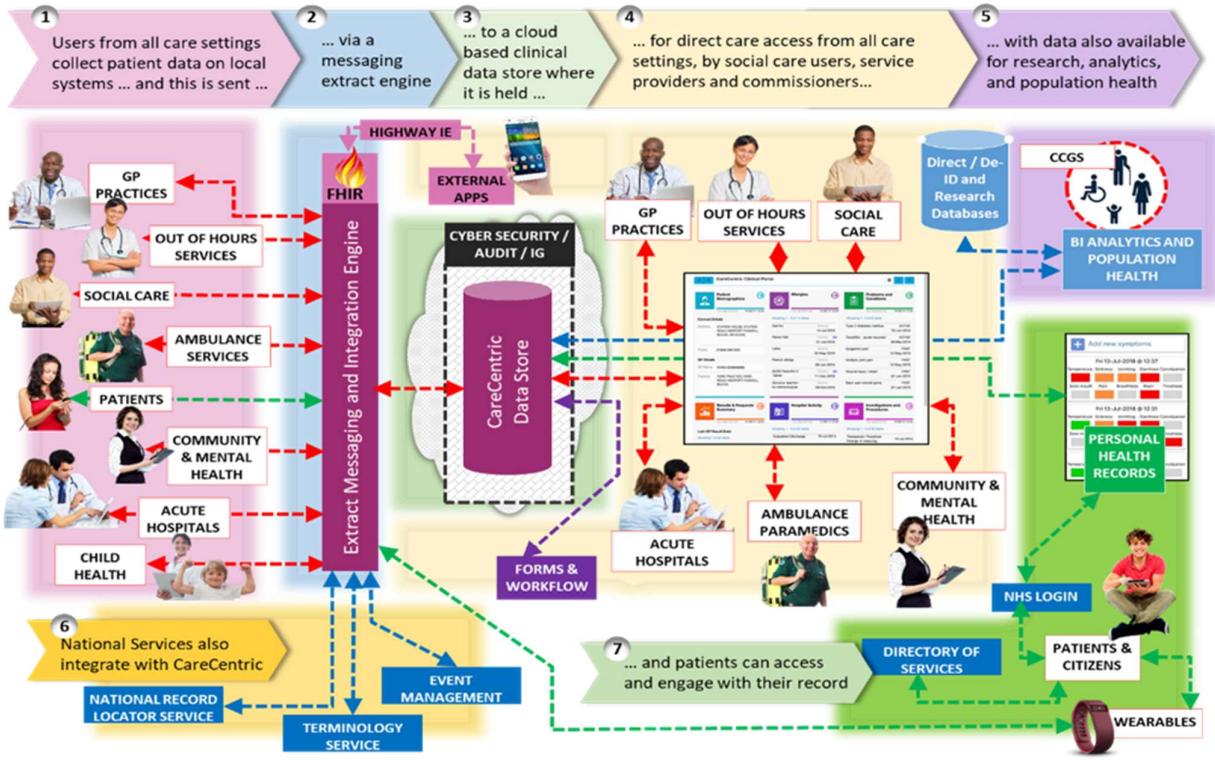
Using our SCR and PH solutions together for the purposes of direct care is very powerful. Case Finding tools in PH are used to identify cohorts of patients who can be surfaced in the SCR in a dashboard as candidates for a care plan and care co-ordination or remote monitoring. If selected the care plans are created and managed in the Shared Care Record as illustrated below;

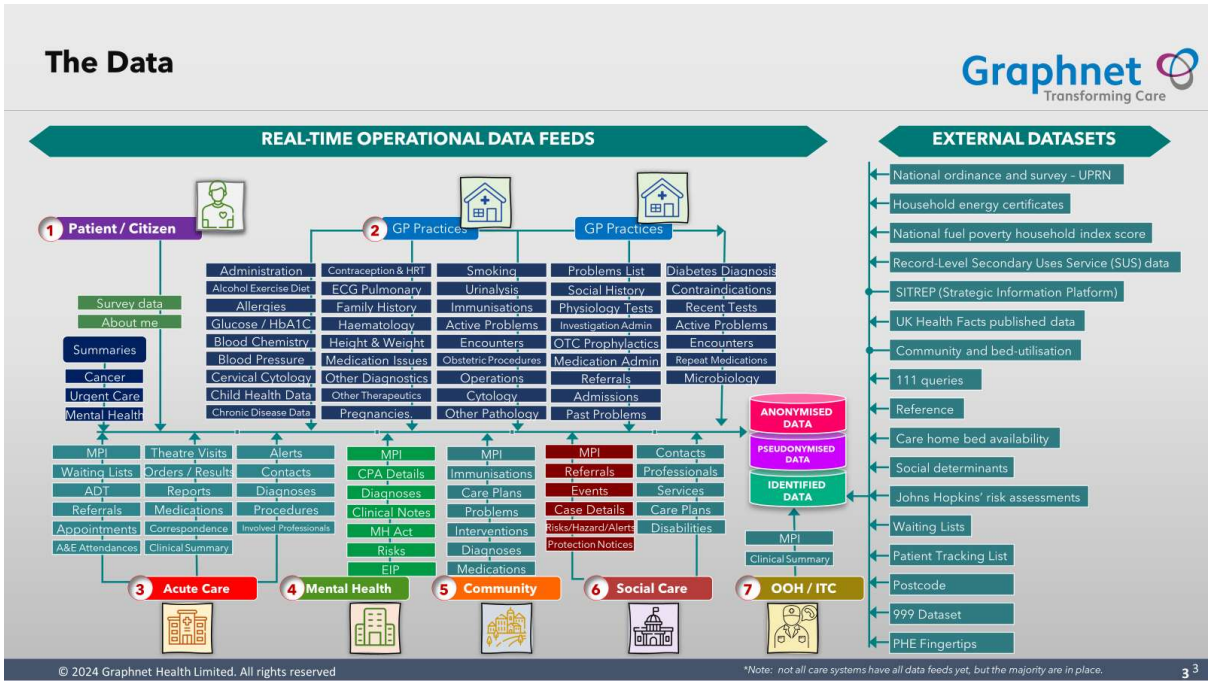
In some instances, the patient can see their care plan via our patient portal (PHR), and it may also be that they are enrolled onto a remote monitoring programme,- the data from which is visible in the shared care record and used in our population health solution.

This is an important and unique aspect of the Graphnet solution set. It is an integrated end to end solution comprising;-

1. Population Health Analytics for case finding and cohort identification for direct care.
2. A Shared Care Record that supports the enrolling of cohorts onto programmes and the management of those patients and programmes.
3. Remote monitoring to support programmes of focused support.
4. A Patient App to enable patients to see, interact with and update their care record.
5. A Single Patient record where data is available all in one place from across many health care settings including but not limited to Primary/Secondary Care, social care, mental health, councils etc.
6. Data Science driven benefits analysis to complete the loop to understand using the single patient record data if an intervention makes a positive impact on both an individual patient or cohort of patients.

2.2 The Graphnet Shared Care Record Product Suite





2.2.1 Non-Functional

Graphnet's Shared Care Record predominantly provides a stored extract of source information from external third-party applications. All data is transported using SSL encrypted links and then stored in a secure database, which is hosted in Microsoft Azure cloud. We routinely commission independent penetration testing of our Shared Care Record solution.

Standards

As a long-standing supplier to the NHS, we are committed to complying with all relevant national standards and guidance, as well as legal and legislative requirements to ensure the safety and security of data. In the UK these include:

- ISO 27001
- ISO 9001
- Cyber Essentials Plus
- DCB0129
- Medical Devices and Software as a Medical Device (SaMD) products under our Graphnet Remote Monitoring offerings are ISO 13485:2016 certified and CE-certified Class IIa Medical Devices under the Medical Device Regulation (MDR) EU 2017/745 managed through Luscii.
- NHS Data Security and Protection Toolkit

We are also compliant with PRSB standards and EPaCCS SCCI5180 for our Integrated Care & Support Plans and End of Life planning.

All our solutions comply with NHS standards and best practice guidelines, including NHS Information Governance standards, e.g. the NHS Confidentiality Code of Practice and Caldicott Principles as defined in the Caldicott Manual.

We are compliant with the HSCN Connection Agreement and the Data Security and Protection Toolkit.

Graphnet complies with the Data Protection Act 2018 and UK GDPR.

Security & protection

Pen test

- Graphnet has a programme of annual independent penetration testing by CREST and National Cyber Security Centre (NCSC) CHECK certified testers and internal vulnerability scanning, incorporating the OWASP “Top Ten” (OWASP10) principles.
- Any “critical” or “high” areas of concern uncovered by a test are scheduled for remediation as a priority. Other items are evaluated and scheduled in too.

Security Operations Centre (SOC)

- The application is monitored using Microsoft’s Sentinel and Security Centre policies, with alerts raised for anomalies found, including suspicious or potentially malicious activity. Audit logs are retained for all Azure, web application and SQL server activities for 90 days. The application keeps its logs indefinitely.
- These audit alerts generate a notification to our specialist 24/7 Security Operations Centre (SOC) who will triage and escalate to the company’s Cyber Security team as required. This may further trigger the incident response process, if appropriate.

Architecture

Encryption

- Data in transit between end user device(s) and the application, within the application and between the application and other services (e.g. APIs) are protected using TLS 1.2.
- Transport Layer Security (TLS) 1.2 (or later) is an industry standard protocol with 2,048-bit RSA/SHA256 encryption keys, as recommended by CESG/NCSC.

RBAC

Web Application Protection

Graphnet deploys the Cloudflare application security service across all customer systems. This is an industry leading UK hosted service that will provide enhanced protection of customer data against increasingly sophisticated Internet based threat actors covering the following:

- DDOS (Distributed Denial Of Service) protection covering layer 3, 4 and 7 attacks. DDOS is an attack where many Internet servers seek to overwhelm a WEB service and disrupt it
- Rogue BOT protection, a BOT will scan the Internet looking for and cataloguing WEB services and vulnerabilities to exploit as the prelude to an attack

- WAF (Web Application Firewall) functionality based on the 'OWASP Top 10', a WAF protects a WEB service from malicious exploits and attack
- Cross-site scripting prevention. Cross-site scripting allows an attacker to inject malicious code into a user's browser using an innocent website, allowing the attacker access to data held in the browser
- Zero-day vulnerability protection. Zero-day vulnerabilities are ones where the details of the vulnerability in software, or hardware, have been released, a patch or fix is not yet available meaning the vulnerability could be being actively exploited by malicious actors
- Cloudflare product is deployed at the perimeter of Graphnet's infrastructure, but is independent of it thus providing a solid firewall to the application infrastructure

Separation between customers

Each customer's application is contained within its own Azure subscription and is therefore isolated from other customers. The management of the application is also separate.

Operational security

Vulnerabilities

- To identify new threats Graphnet monitors NHS CareCERT, US-CERT and other industry sources for intelligence regarding threats, vulnerabilities and exploits. These are assessed weekly and any high-risk ones may be subject to emergency patching or action.
- Vulnerability assessments of the application and its components are performed within Azure, and any findings are investigated and appropriate (if any) remedial actions taken.
- Vulnerabilities are managed through a cycle of regular patching for the IaaS elements within 14 days of the patches being made available. The Microsoft Azure platform handles the patching of the hardware infrastructure and PaaS components. Any critical patches or fixes will be applied according to the suppliers' guidelines.
- For other vulnerabilities and threats to application and software components that Graphnet manage, an incident ticket is raised, and the board of directors are notified automatically. A security expert will assess and Risk Score using Impact and Likelihood, with Impact based on the possible impact on confidentiality, integrity and

availability. The Risk Score is used to prioritise mitigations. The PaaS components and underlying hardware are under Microsoft's management.

Incident management

- Any staff member who becomes aware of a security incident/near miss, an error that may have been made by the information systems or, physical access to the office/equipment, must formally report such errors to their line manager as well as raising an incident ticket as laid out in GN BMS-DOC 007 Security Management and Risk Assessment Policy.
- An incident/near miss, error that may have been made by the information systems or irregular physical access to the office/equipment, is reported either by employees or protective monitoring.
- An appropriate Jira service desk ticket is raised to notify the IG/IS/ISO management team, who will discuss and allocate the investigation and management of the risk.
- The seriousness of an incident is not the main issue; even minor ones (or 'near misses') may be symptomatic of a deeper and much more serious problem and all staff are encouraged to flag anything suspicious.
- A two-tier system is in place to respond to security incidents: the IG/IS and ISO management team will assess issues and monitor progress on the action taken to ensure corrective action is taken. The Cyber Incident Response Plan (CIRP) will be activated as part of our Major Incident process if we suffer an attack, intelligence suggests an attack may be likely or a threat or vulnerability is "critical" as indicated by its CVSS score.
- Minor incidents/issues shall be raised on JIRA GQS service desk and allocated an individual reference number: any employee may add an issue.
- The management team will close the issue/incident when satisfied that acceptable corrective action(s) has been taken
- Escalation of a ticket directly to senior members of the Governance Board will be used for significant issues. These will be progressed and closed as detailed below.
- The IG/IS/ISO management team will monitor investigations and actions taken to ensure appropriate corrective action is taken, e.g. update policies/procedure, risk assessment, IaaS or software fix.

- When the management team, and where required the SIRO, is satisfied all possible actions have been taken, the issue shall be resolved and the mitigation plan assessed for success for closure.
- In the event of the CIRP being invoked then the incident will be managed by the Computer Security Incident Response Team (CSIRT) with additional resources included as necessary.
- All potential impacts and risks (financial, public perception, confidentiality etc.) are considered when a risk incident is reported. As the contractual Data Processor, Graphnet will notify the customer (Data Controller) within 24 hours. The Data Controller however must make its own independent assessment and make the decision to report to the ICO.

Governance

- Graphnet has a defined Governance Framework, including:
    - Risk Management Framework;
    - Governance Board for data and service risk ownership.
- These are supported by the following:
    - Senior Information Risk Owner (SIRO);
    - Chief Technology Officer
    - Director of Information Governance;
    - Legal Counsel;
    - Information Security Manager;
- The board has access to the company's Risk Register and board members attend regular meetings of the Security Board.
- Graphnet hold the ISO 9001, ISO 27001 and Cyber Essentials Plus accreditations. The company and applications are compliant with these standards and is tested annually for them. The company also completes the Data Security and Protection Toolkit annually.
- Graphnet has a full range of internal data security and governance policies covering the full scope of ISO 27001.
- The Information Security Manager works on a day-to-day basis with IG, compliance and legal teams to ensure compliance.

Supply chain management

- Graphnet ensures its partners' and sub-contractors' contracts cover non-disclosure, Information Governance and Security.
- Security Risk assessment will be undertaken of third-party suppliers using the Standard Templates which form part of the ISO 27001 database.
- Any sub-contracts are agreed on a back-to-back basis which includes a flow down of the customer's contract and tender requirements (to the extent they apply to the sub-contracted services being supplied).
- Customer data are not shared with third party suppliers without the customer's explicit agreement and controls are in place to prevent any customer data from being visible or transmitted outside the United Kingdom.

Secure development

- Graphnet follows the Scaled Agile Framework for Enterprise (SAFE), and all source code is managed by industry standard source control systems.
- The software development process is governed by the "GN BMS-DOC 015 Secure Software and Solution Development Procedures" document that covers secure development and testing, and the application deployed in accordance with the Release Management Policy audited to ISO 27001.
- Graphnet have developed FHIR APIs in alignment with UK Core FHIR standards from NHSE, are ITK compliant and have signed up to the Tech UK Interoperability Charter.

Operations

Graphnet follows a standard ITIL deployment methodology which includes: Change Advisory Board; Release Documentation; Release Management Control; Capacity Management; Impact Assessment; User Acceptance Test and Customer sign off. We have also adopted Scaled Agile Framework (SAFe), which employs an AGILE methodology for software development and patch releases.

Our Service Desk provides a second line incident triage and helpdesk service and operates to ITIL principles, reviewing incidents and identifying problems in accordance with internal protocols. We use an ITIL focused call logging application (JIRA) to record details of all fault

calls and support incident management.

3 Details of the level of backup/restore and disaster recovery that will be provided

Graphnet employs a multi-layer approach to Business Continuity and Disaster Recovery for the cloud hosted Graphnet Shared Care Record solution. We have a well-developed, formal Business Continuity and Disaster Recovery plan, which has been audited as part of our ISO9001 and ISO27001 accreditations and reviewed annually. This plan identifies key resources and contingencies required in the event of a major incident and the preparation and alternatives in place allowing business to be run during the restoration of full services.

Graphnet manages Disaster Recovery (DR) and Business Continuity (BC) arrangements in a structured manner. A DR Plan is in place for every system or product for which there are contractual Disaster Recovery arrangements in place with customers. Business Continuity plans exist to ensure that in the event of a disaster affecting the company's essential business functions, we will be able to continue with standard operations expected by customers. Annual testing and review of both DR and BC plans takes place.

We deploy our services in Microsoft Azure, a resilient cloud-based platform, which allows for multiple layers of resilience and high availability across multiple physical datacentres. The platform meets many industry hosting requirements outlined for NHS Applications, Services and Data. Accreditations and standards achieved: include Level 2 NHS IG Toolkit assessment; UK Government's Cloud Security Principles; ISO 27001, ISO 27018, HIPAA, FedRAMP, SOC 1 and SOC 2.

Using Microsoft Azure platform-as-a-service (PaaS) technologies, we leverage many of the multi-zonal capabilities provided which publish SLA levels of availability of 99.999%. Regarding data protection, the Azure storage resiliency solutions which are part of the core Azure platform, provide storage and data availability to 99.99 (12 9s) to support strict RTO and RPO requirements. To add an additional layer of resilience, we deploy a full replica of infrastructure, software and data to a paired Azure region – ensuring our systems are not disrupted by Azure fabric updates. In most cases, this also allows us to failover and restore service quickly with minimal disruption, giving us the ability to remediate the original fault in the background whilst

the service is operational to end users.

We utilise the Managed backup services as part of Azure SQL, which consists of full database backups weekly, differential database backups generally taken every 12 hours, and transaction log backups every 5 - 10 minutes to protect your business from data loss. Recovery time depends on several factors including the total number of databases recovering in the same region at the same time, the database size, the transaction log size, and network bandwidth. In most cases, recovery of service is as simple as a failover to the paired region database, which doesn't require any restoration from backup. We can then work on recovering and re-introducing the faulting node in the background without service impact.

In the case of data corruption, we would restore an existing database from the automated backups to an earlier point in time as a new database, then use scripts of services like Azure Data Factory to delta the desired data back into the main database. Azure database backups are immutable, and the files are not accessible directly – protecting them from things like Ransomware attacks. Data retention policies are also in place to protect the backups should the databases or database servers get removed.

Should the absolute worst happen and some of the infrastructure is removed or corrupted beyond repair, all our infrastructure is deployed using automated pipelines via Infrastructure as Code (Terraform) modules, ensuring we can redeploy back to a known-good state with a high level of confidence.

4 On-boarding and Off-boarding processes

4.1 On-boarding

Configuration

Graphnet has developed a standard configuration for the Graphnet Shared Care Record based on our experience, national standards and through engagement with our many customers. This standard configuration can be tailored to suit the local requirements of each customer during deployment. We have a standardised approach to collaborating with our customers to achieve the configuration required in a timely and efficient manner. To complement this, Graphnet will also assist and support the customer in aligning/realigning their business processes to help enable them to maximise the benefits from the use of the solution.

Dependent on the agreed scope of the contract, configuration options can include:

- System Security and Login preference settings, including password management.
- Data feed configurations.
- Data mapping configurations.
- System settings and permissions.
- Selection and drop-down lists.
- Role-Based Access (RBAC) and Consent Model configuration.

Data Migration

Most Graphnet Shared Care Record installations require an element of data migration/extraction; for the purposes of the creation of the initial baseline MPI, using Acute and GP demographic data. This can be further augmented with demographic data from other systems, e.g., community. Graphnet has a team of experienced data migration specialists who work with our customers to fulfil this activity during implementation.

We will work closely with the customer to establish and agree the following:

- The scope of the work required.
- Individual and joint responsibilities within the workstream.
- The plan and optimum phasing of activities.

4.1.1 Important Note

Please note that we have included our standard implementation charges within the Pricing Document for transparency and indicative budgeting. However, due to the very specific and individual nature of each project and the fact that every customer's requirements, environment, and delivery approach can differ these standard charges should be treated as a baseline only. A full and accurate implementation cost will be confirmed following detailed scoping and agreement of the final project requirements, as it is not possible to apply a single fixed fee to these critically important services.

4.2 Off-boarding

At the end of the contract term, Graphnet will work with the Buyer to agree an exit plan. As a responsible provider, Graphnet is aware of our obligations regarding the management and retention of data, both during the term of the contract and when the contract concludes. The shared record system is replicating or re-presenting data which is held in other source systems (such as an Acute PAS or GP system). These are the master systems holding the original data and we understand that the data in these systems must be protected at contract end.

5 Service Management Details

We provide a second line incident triage and helpdesk service, using our centralised, expert team who provide support remotely. The Support Desk operates to ITIL principles, reviewing incidents and identifying problems in accordance with internal protocols. Customers provide a first line help desk and third line support is provided internally by our development, TechOps and DevOps team.

We use an ITIL focused call logging application (JIRA) to record details of all fault calls and support incident management. Incidents can be reported online and progress can be monitored online or follow up by telephone.

We also have experience of managing support calls that require escalation/pass through to a 3rd party organisation.

We will agree a Service Level Agreement with new customers and this, typically, covers the target response times for genuine faults with the application. Our Service Delivery Executive, along with our Account Executive will conduct regular reviews with individual customers related to the performance of the Service Desk. Reviews will cover all incidents raised and will provide regular reconciliation reports and progress updates. The SLA will cover the support and maintenance offered.

Our service desk will be responsible for the monitoring of SLAs for response, closure of calls logged and reporting of associated statistics.

5.1 Incident Management/ Problem Management

Graphnet uses JIRA™ incident management software to manage its Service Desk and track all reported software issues and change requests.

Issues and requests can be logged via the JIRA online portal. Buyers provide an agreed minimum specification of supporting information in order that we can act upon and provide resolutions to issues raised efficiently. Issues raised are prioritised and allocated a unique reference number

to facilitate tracking and management. If calls need to be referred to third party support (for example to Microsoft or other system software which is used in our solution), Graphnet will maintain responsibility for monitoring the progress of the call until closure.

Regular service review meetings are undertaken with Buyer and Graphnet representatives, including the Buyer's appointed Service Delivery Executive, to monitor Service Levels, review problems, understand root cause analysis and manage any process issues between desks.

5.2 Change Control

Graphnet has a standard Change Control process based on ITIL principles. The full process and governance for managing and approving change requests is documented in the Project Initiation Document. The JIRA case management system is used to log change requests. This is typically done by the Buyer's appointed Service Delivery Director, who will also track and manage requests and updates on the Buyer's behalf.

Graphnet has a mature process for dealing with change requests. If an improvement to the existing product set is identified, or there is a request for change in scope for the project, then a request can be made through the submission of a Change Request Form. Graphnet assesses all Change Requests for clinical usefulness, clinical safety and fit with product vision or strategy. The request will be reviewed and assessed, with full details and associated costs/timescales fed back as promptly as possible.

Our development is carried out in an Agile environment, which allows for a more flexible and responsive design, development and testing approach, enabling rapid release of requested changes.

5.3 The Role of the User Groups

Our user community is heavily involved in influencing our development roadmap. There are several mechanisms for our end user community to influence the future development of our solutions. These include:

- User groups/clinical forums open to all customers
- Change requests
- Data driven roadmap planning
- Opportunities for customers to influence the strategic direction of the product
- User experience research and feature request process
- The ability to recommend changes to the product.

5.4 Software Upgrades

Graphnet provides a full Release Management Service as part of its Change Control process and has formal procedures in place to ensure control over the release of all versions of its software, and these comply with ISO 9001 and TickIT standards.

It also follows standard ITIL framework processes. All patches are tested internally prior to deployment and are monitored for success. Customers are provided with comprehensive Release Notes to accompany releases, detailing all fixes and changes to support their own UAT. The release is tested by the customer and accepted for live use. The release is then scheduled for promotion to live. Documentation for the release adheres to principles in use as part of our accreditation to the ISO 9001 quality standard.

6 Service Constraints

Each of the core and optional elements of our solution are described in Section 1 of this document and outlined in the accompanying Pricing Information. The service provided will include the current release of the elements of the Shared Care Record solution contracted for use by the customer.

Our solution pricing is based on standard, core configuration and “out of the box” functionality consistent with the latest product releases.

We can provide a full range of implementation services, which will be specified and priced upon request. This includes the following implementation services:

- Programme and Project Management.
- System configuration and functional/product expertise.
- Data migration.
- Integration and interfacing.
- Training.
- Management information and reporting.
- Change and benefits management.
- Other services and resources such as go-live support and temporary customer-side resources.

Planned downtime is kept to a minimum, usually needed only for new major Release Updates.

Graphnet will always plan and agree such scheduled downtime with the Buyer in advance.

7 Service Levels

7.1 Availability

The hosted server environment we deploy is a resilient cloud-based Microsoft Azure platform, which allows real time mirroring of software and data. This a platform already being used to host UK SCR's and meets hosting requirements outlined for NHS Applications, Services and Data. Accreditations and standards achieved include Level 2 NHS IG Toolkit assessment; UK Government's Cloud Security Principles; ISO 27001, ISO27018 (planned), HIPAA, FedRAMP, SOC 1 and SOC 2. Microsoft Azure Availability Sets and Availability Zones, which we would propose for our customers cloud-based solution, support published SLA levels of availability of 99.99%. Regarding data protection, the Azure storage resiliency solutions which are part of the core Azure platform, provide storage and data availability to 99.99 (12 9s) to support strict RTO and RPO requirements.

The Azure SQL Database includes mechanisms, policies, and procedures that enable the business to continue operating in the face of disruption, particularly to its computing infrastructure. Azure automatically performs a combination of database backups to protect your business from data loss. The backups are stored in RA-GRS storage for 35 days for all service tiers except Basic DTU service tiers where the backups are stored for 7 days.

7.2 Performance

Graphnet provides a dashboard showing incidents, usage and availability, which support performance, incident and response monitoring and reporting as part of our comprehensive Service Management package included within our contracts.

As part of this service, we provide:

- Active monitoring of the solution performance, faults and availability.
- Monitoring of and support for all interfaces.
- System performance is reported to Buyers as part of regular Service Review meetings and formal monthly reporting.

7.3 Incident response and resolution

Our aim is to respond to incidents quickly and effectively and to resolve incidents as quickly as possible to avoid the disruption and difficulties which such incidents may cause. Full details of response and resolution are detailed in the Graphnet Service Level Agreement.

Example SLA response and resolution times:

Priority Level	**Service Level Performance Criterion**	**Service Level Performance Measure** (Target Response, Investigation and Resolution Times)
P1 (Critical)	Entire system unavailable or unusable. Or An issue identified as having significant operational (e.g. clinical) risk with no acceptable work-a-round	Automatically logged immediately. Triaged and initial response within 15 minutes during Working Hours. Investigated and notification of planned action within one (1) Working Hour. Resolved within four (4) Working Hours
P2 (High)	Significant loss of the service but the impacted business function is not halted. An issue identified as having potential to cause operational (e.g. clinical risk) with no acceptable work-a-round.	Automatically logged immediately. Triaged and initial response within 15 minutes during Working Hours. Investigated and notification of planned action within one (1) Working Hour. Target Resolution Time - Resolved within eight (8) Working Hours.
P3 (Medium)	Reduced capacity of the service, a key module or major function but with a small impact on the business operation.	Automatically logged immediately. Triaged and initial response within 15 minutes during Working Hours. Investigated and notification of planned action within four (4) Working Hours. Target Resolution Time - Resolved within one hundred and twenty (120) Working Hours.

P4 (Low)	Intermittent or partial faults resulting in loss of noncritical functionality where the software is still useable or there is a suitable alternative. Cosmetic issues that have limited impact.	Automatically logged immediately. Triaged and initial response within 15 minutes during Working Hours. Investigated and notification of planned action within eight (8) Working Hours. Target Resolution Time - Resolved within twenty (20) Days

7.4 Support Hours

The standard Period of Support covers the hours from 09:00 to 17:30 Monday to Friday excluding all Bank Holidays. We also offer extended support hours or 24x7 as a further service subject to additional charges.

8 Training

Our training methodologies have continually evolved over our 25 years of experience, supporting care providers in their implementation of our range of products. Our approach to enabling the user is through the development of a comprehensive training and engagement programme designed to provide flexible opportunities to hands on learning.

This approach demands early engagement with the stakeholder organisations to fully understand the local training management approach and systems. Our operational processes for software development, implementation, training and support services are certified to ISO9001.

Graphnet will provide a Training environment which mirrors the live use Graphnet Shared Care Record portal; it has several test patients which provide examples of patients and data for training purposes. The nature of our solution footprint is such that building functional environments for the purposes of testing and training etc. can be achieved relatively quickly and using virtualised resources to control cost and improve flexibility. This also means that the data in these environments can be protected and backed up on a semi-live footing. This is important to protect local configuration and test data and to ensure that the project progress is protected.

Our preferred approach is to provide Train the Trainer training, so a customer's staff can then go on to deliver specialist training for end users (including clinicians and other care professionals, as well as for specialist users, such as system administrators,) and to support the customer team in the preparation and early delivery of end user training. These local trainers therefore act as super users within the local organisations.

9 Ordering and Invoicing Process

Our ordering and invoicing process is as follows:

- The Buyer raises a purchase order to cover the charges agreed under the contract or through quoted changes.
- The Buyer and supplier to sign an order form which details the specific scope of the service to be delivered for the Buyer. Graphnet will draft the order form.
- Graphnet invoices the Buyer in accordance with the timescales specified for different components of the services. This will vary from Buyer to Buyer, but under a SaaS model, we will typically invoice the Buyer for the services quarterly in advance, from the date of go-live and until the end of the contract term.
- Buyers may also elect to profile capital payments (for software licences and implementation services) against agreed delivery milestones during the deployment period, with service charges invoiced from go-live as above. Delivery milestones will be invoiced in accordance with completed Milestone Achievement Certificates (MAC's).
- Each invoice is sent to the approved Buyer's address (such as the finance department) and contains appropriate information to identify the element/s of the service to which it relates, including the purchase order reference.
- Invoices shall where necessary be accompanied by sufficient supporting documentation.

10 Payment Terms

Graphnet's standard payment terms are within thirty days of receipt of a valid invoice.

10.1 Disputed Invoicing

If the Customer disputes all or any part of an invoice, both parties should discuss and if appropriate, a credit note and a corrected invoice issued accordingly.

11 Termination Terms

Graphnet offers its customers termination rights in line with industry standards, such as the Buyer's right to terminate should the supplier be in material default, commit a material and irremediable breach of the contract, be insolvent or in default of Protection of Personal Data, Confidentiality or the Security Policy and so on. Our policy is in line with standard government provisions and will be detailed in the contract terms.

12 Data Restoration / Service Migration

12.1 Data Restore

We deploy our services in Microsoft Azure, a resilient cloud-based platform, which allows for multiple layers of resilience and high availability across multiple physical datacentres. The platform meets many industry hosting requirements outlined for NHS Applications, Services and Data. Accreditations and standards achieved include Level 2 NHS IG Toolkit assessment; UK Government's Cloud Security Principles; ISO 27001, ISO 27018, HIPAA, FedRAMP, SOC 1 and SOC 2.

We utilise the Managed backup services as part of Azure SQL, which consists of full database backups weekly, differential database backups generally taken every 12 hours, and transaction log backups every 5 - 10 minutes to protect your business from data loss. Recovery time depends on several factors including the total number of databases recovering in the same region at the same time, the database size, the transaction log size, and network bandwidth. In most cases, recovery of service is as simple as a failover to the paired region database, which doesn't require any restoration from backup. We can then work on recovering and re-introducing the faulting node in the background without service impact.

In the case of data corruption, we would restore an existing database from the automated backups to an earlier point in time as a new database, then use scripts of services like Azure Data Factory to delta the desired data back into the main database. Azure database backups are immutable, and the files are not accessible directly – protecting them from things like Ransomware attacks. Data retention policies are also in place to protect the backups should the databases or database servers get removed.

12.2 Service Migration / Exit

At the end of the contract term, Graphnet will work with the Buyer to agree an exit plan, including the migration of data from the system and the decommissioning of any locally sited hardware (if any) provided under the contract.

13 Buyer Responsibilities

Buyer responsibilities depend on the scope of solution /services being provided. Typical Buyer responsibilities are summarised below:

13.1 General Obligations

- To perform its obligations and provide suitable numbers of suitably qualified staff, as well as access to those staff by the Supplier.
- To provide such documentation, data and/or other information that the Supplier reasonably requests.
- To make available to the Supplier premises, facilities, relevant ICT systems etc.
- To provide suitable on-site accommodation including vehicle access, desk space, telephones and network/Wi-Fi access for the Supplier staff.
- To ensure all relevant information governance and information security processes, agreements and controls are in place.

13.2 Management and Direction

- To adhere to the PRINCE2/ recognised project management methodology.
- To provide a programme manager, one or more project managers and a range of staff (the job roles for which will be agreed in advance) to undertake a range of tasks and roles (agreed in the contract) covering both the implementation period as well as the live usage period to the end of the contract term.
- To agree appropriate joint project governance with the Supplier and to ensure senior level input (including clinicians) to the Project Board.
- To provide staff during the implementation period who will be responsible for the design, configuration and build (under the guidance of the Supplier), and for the subsequent operation and maintenance, of elements of the Supplier Software.

13.3 Testing and Acceptance

- To evaluate the Supplier Software to ensure that it meets user requirements in accordance with the agreed Testing.
- To provide sufficient testing resources to undertake UAT and other Buyer testing as required.
- To develop and document Test scripts.

13.4 System Management

- To provide skilled resource(s) to undertake system administration of the system on behalf of the Buyer.
- Housekeeping tasks including setting up of new users and their access rights.
- To make available to Buyer's staff copies of the correct operating instructions for proper use and care of the Supplier Software.
- To ensure remote access to the System is always available for the Supplier and its Sub- contractors.
- To actively scan and monitor for suspicious events and virus control according to the Security Management Plan.

13.5 Support Services

- To provide 24x7 first line support and second line help desk support services.
- To collect the necessary minimum data and/or supporting information required for the identification, replication and resolution of faults and to have the necessary training and skills to enable problem identification between hardware, network and application so that the call can be resolved internally or logged with the appropriate supplier.
- To ensure that calls are logged and passed to the Supplier via approved methods and to maintain a log identifying the date and time logged, priority and current status.
- To make the Supplier aware of all local changes affecting the operation of the system including system configuration and technical infrastructure changes; and
- To provide a point of contact to interface with the Supplier in relation to the performance monitoring system including involvement in service reviews.

13.6 Infrastructure, Networking and end user Devices

- To provide the necessary local networking infrastructure. This includes the communication points and authorisation for remote access to servers from the Supplier's designated access points.

- To provide an Active Directory domain and to ensure that this is accessible to all remote locations and networks required to access the Supplier Solution as well as ensuring that it integrates with the server-based AD domain.
- To ensure system security and the control of system access.
- To provide all necessary end user devices, PCs, laptops, mobile devices, peripherals, printers, print servers and bar code scanners, including configuring the Supplier Software to access such devices.
- To provide end user workstation to an agreed minimum specification, and to agree to update the minimum specification from time to time in line with the necessary technological development required for improved functionality to be incorporated into the Software and to preserve its supportability.
- To identify and plan for Supplier's personnel to avoid or be protected from any health hazards and to take all reasonable precautions to protect the health and safety of the Supplier's personnel whilst on the Buyer's premises.

13.7 End User Training

- To provide and host all end user training including any general PC skills training as well as training on the Supplier's Applications, both during the initial implementation and thereafter, and to ensure that the correct staff attend the courses.
- To provide suitably experienced Trainers to attend the Supplier's "Train the Trainer" training sessions.
- To localise and customise the standard training materials provided by the Supplier.

13.8 Data Migration

Most Graphnet Shared Care Record installations require an element of data migration/extraction; for the purposes of the creation of the initial baseline MPI, using Acute and GP demographic data. This can be further augmented with demographic data from other systems, e.g., community. Graphnet has a team of experienced data migration specialists who work with our customers to fulfil this activity during implementation.

We will work closely with the Buyer to establish and agree the following:

- The scope of the work required.
- Individual and joint responsibilities within the workstream.
- The plan and optimum phasing of activities.

13.9 Interfacing and Integration with Legacy Systems

- To provide and operate interfaces between the Buyer's legacy applications and the Buyer's integration engine and the Supplier's integration engine, including the provision of suitable test environment/s.

To provide the following interfacing support services:

- first line support to triage the problem to diagnose where the problem lies (i.e. on which side of the interface) should an interface stop or not be working satisfactorily
- communicating the fault to the Supplier using the standard helpdesk procedures; and
- ensuring that no changes (such as upgrades) to the Buyer's legacy systems adversely affect the interface to the Supplier Software and if this is likely then to notify the Supplier in a timely way so that necessary work and testing can be undertaken under the Change Control Procedure.

To procure for the Supplier.

- access to any legacy system/s with which the Supplier Software interoperates, and to bear any third-party costs associated with this.
- Be responsible for ensuring that data sharing agreements and associated information governance requirements are met so that any patient identifiable data shared with the service is done so with the correct approvals, consent and sanctions.
- Agreements as to the patient consent model with appropriate governance bodies.

14 Technical Requirements

Graphnet will discuss individual Buyer requirements (on a case-by-case scenario) regarding all technical specifications, as this will be dependent on the scope of the project and the number of organisations contributing to the shared care record. A basic guideline to minimum requirements is stated below but is only given as a guideline and would be subject to review with the Buyer.

Software & Screen Resolution:	Minimum 1280 x 1024 capable display
	1920 x 1080 preferred
	Microsoft Edge (Chromium, not including use in IE Mode) Google Chrome Firefox
	It is recommended that customers set their screen resolution to 1280 x 1024 for optimal viewing. For SSO/Embedded users of Graphnet Shared Care Record , the minimum supported screen resolution is 1280 x 1024. The window/screen space available to Graphnet Shared Care Record for SSO/Embedded users must be at least 1024 x 768 or some functionality may not be available.

14.1 Details of any trial service available

Trial services of the Graphnet Shared Care Record solution and other products described under the G-Cloud framework are available where practical. For example, if a potential customer wishes to see a system with real life data in it imported from GP systems and Acute systems, it would incur considerable 3rd party cost from them and us to facilitate this so it may not be practical, but if a test version of the product was adequate with dummy data then we can facilitate that.

14.2 Sub-Contractors

Graphnet has the necessary and appropriate products, services, experience and skills to provide, implement, host and support the implementation of the Graphnet Shared

Care Record solution. Should the Buyer have specialist requirements not met by Graphnet's products and services portfolio then we would expect to sub-contract such services as required. Graphnet has several years' experience in managing sub-contractors in this manner to meet contractual requirements.