

Health Informatics Cloud

Lot 2b: Software as a Service (SaaS)

Contents

1. Description of Service
2. Features and Benefits
3. Implementation Plan
4. Information Assurance and Security
5. Ordering and Invoicing Process
6. After Sales Support and Services Levels
7. Business Continuity and Disaster Recovery Plan

For further information:

☎ +44 (0)20 7602 6000

✉ digital.marketplace@caci.co.uk

🌐 www.caci.co.uk

1. Description of Service

Summary

Health Informatics Cloud (HIC) is a secure cloud data platform with modular applications that help NHS providers and health boards turn raw data into operational and financial insight. HIC accelerates analytics delivery, supports privacy-preserving data sharing, and reduces time to value by providing a managed foundation with optional apps such as costing analytics and maternity insights. It is designed to advance common UK health system agendas: integrated care and collaboration, recovery and operational performance, financial sustainability and productivity, robust data and digital foundations, population health and prevention, quality and safety, workforce enablement, and transparent, auditable reporting. HIC also supports Provider Collaboratives by enabling pathway analytics and governed data sharing that transcend organisational boundaries. In addition, HIC interoperates with Federated Data Platform (FDP) products to help providers adopt FDP while maintaining coherent, reconciled analytics across both platforms through standards-based integration and shared semantic models.

Who is it for and typical outcomes

- NHS Trusts, Health Boards and regional programmes that need a scalable cloud analytics platform with ready-to-use healthcare data models and apps.
- BI, Finance and Clinical teams who require governed self-service access to trusted data.

Outcomes: faster time from ingestion to insight; improved cost and activity visibility for productivity and financial sustainability; operational performance support across elective recovery and urgent and emergency care; pathway analytics for Provider Collaboratives that transcend organisational boundaries with governed, cross-organisation data sharing; stronger data and digital foundations and interoperability; population health and inequalities insight; proactive quality and safety monitoring; reduced manual effort through self-service analytics and automation; consistent, auditable reporting for transparency and accountability.

2. Features and Benefits

Alignment with Healthcare Agendas

- Integrated care and collaboration: enable cross-organisation data sharing and ICS/region-level insight to coordinate care pathways and reduce fragmentation.
- Recovery and performance: support elective recovery, urgent and emergency care flow, and reduction of unwarranted variation with timely operational analytics.
- Financial sustainability and productivity: provide trusted cost and activity insight to inform efficiency, value-based decision-making and medium-term financial planning.
- Data and digital foundations: standardise ingestion, metadata and governance to accelerate safe reuse of data, improve data quality, and meet interoperability expectations.
- Population health and prevention: surface population-level views, inequalities analysis and outcomes tracking to target interventions and monitor impact.
- Quality and safety: enable proactive monitoring, incident trend analysis and assurance reporting with auditable access controls.
- Workforce enablement: reduce manual processing, support self-service analytics, and free specialist time for higher-value work.
- Transparency and accountability: deliver consistent metrics and repeatable reporting to meet national planning and performance requirements.
- Security, privacy and IG: apply privacy-preserving controls, UK data residency, and role-based access to meet information governance expectations.

Included Features:

- Managed cloud data platform foundation with healthcare-oriented data structures.
- Modular applications (for example, costing analytics, maternity insights) that plug into the platform.
- Governed data access aligned to organisational roles and responsibilities.
- Standard data ingestion patterns and connectors for common NHS data sources.
- Interoperability with Federated Data Platform (FDP) products to support provider adoption, with standards-based integration and shared semantics for coherent analytics across both platforms.
- Privacy-preserving data handling including role-based access controls and encryption in transit and at rest.
- Operational dashboards and semantic models to accelerate reporting in common BI tools.
- Documentation for onboarding, operations and routine updates.

Excluded:

- Bespoke application development beyond configuration of the listed modules.
- Non-cloud hosting or on-premises deployment.
- Buyer's cloud consumption charges and third-party software licences.
- Data entry or remediation services outside agreed onboarding tasks.

3. Onboarding and Offboarding

Prerequisites and dependencies

- Buyer cloud tenant and identity provider (for example, Microsoft Entra ID) with federated SSO support.
- Access to required data sources and extract schedules.
- Named service owner and technical contact for approvals and change control.

Onboarding approach and indicative timelines

- Discovery and readiness checklist completion.
- Tenant connection, identity integration and baseline security review.
- Data connection setup and validation using sample datasets.
- Enable selected modules and publish initial reports.
- Knowledge transfer for administration and routine operations.
- Typical onboarding for a single organisation with one initial module can complete in weeks, subject to data availability and buyer approvals. A detailed plan is provided at call-off.

Approach - Fusion Methodology

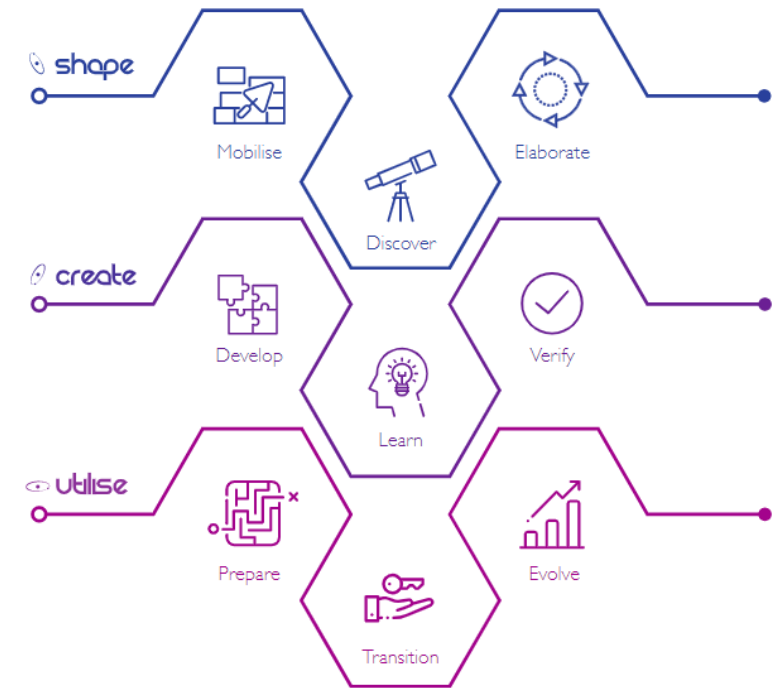
Our onboarding and implementation methodology is built on three pillars of delivery:

- Shape - establishing the vision and foundations of the project, its structure and its governance, to afford clarity.
- Create - ensuring that together, we build the project in the way that you need it to be built.
- Utilise - setting your new solution live and building for the future.

Exit and data portability

Standard and open data export mechanisms and documentation provided.

Support for de-provisioning and knowledge handover at the end of the call-off term.



4. Information Assurance and Security

Summary

CACI's Health Informatics Cloud (HIC) is designed with robust security and compliance at its core. The platform is accredited to ISO27001, ISO9001, and Cyber Essentials Plus standards, ensuring data is encrypted both in transit and at rest, with UK data residency options available. Role-based access and least-privilege principles are enforced, aligning with NHS information governance and the National Cyber Security Centre's cloud security guidance. Security controls include privacy-preserving measures, regular audits, and compliance with the NHS Data Security and Protection Toolkit. Artefacts and evidence of compliance are available on request, supporting transparency and assurance for all stakeholders.

Key Security features included:

- Accredited to ISO27001, ISO9001, and Cyber Essentials Plus
- Data encrypted in transit and at rest
- UK data residency options
- Role-based access controls and least-privilege principles
- Privacy-preserving data handling and pseudonymization by default
- Compliance with NHS Data Security and Protection Toolkit
- Regular audits and alignment with NHS and NCSC cloud security guidance
- Artefacts and evidence of compliance available on request

5. Ordering and Invoicing Process

CACI PRIDES ITSELF IN BEING EASY TO DO BUSINESS WITH

With this in mind, we take an Agile approach to all our engagements, working closely with customers and their stakeholders to design and deliver cloud services in an iterative manner. This enables us to meet specific requirements as well as delivering value and benefit for our customers as early as possible.

Prior to the delivery commencing, our Engagement Manager will work with the customer to agree the outcomes for the engagement, including:

- Defining the success criteria and ensuring the commercials align
- Agreeing specific deliverables for the engagement
- Agreeing the specific ways of working and governance for the engagement
- Understanding the security constraints and ensuring the relevant clearances are in place
- Defining and agreeing the team size/resourcing required
- Putting the commercials in place in line with the G-Cloud framework.

We will then produce a proposal which contains a Services Supply Agreement, detailing the scope of work and the associated price. For details about our standard invoicing process, please refer to the Terms and Conditions document.

6. After Sales Support and Service Levels

ITIL STYLE SUPPORT

Service Levels - Detailed Overview

CACI's support service for the Health Informatics Cloud (HIC) is structured around ITIL principles and is designed to be flexible, reliable, and responsive to customer needs. Service is primarily delivered remotely, with on-site support available by agreement. The standard support window is Monday to Friday, 9am to 5:30pm (excluding UK bank holidays), but can be tailored by contract.

Incident Management and SLAs

- All incidents are logged and tracked in a CRM system, with clear status updates and historical records for analysis and improvement.
- Incidents are categorised by severity, which determines the target response and resolution times:
 - **Severity 1 (Critical):** 1-hour response, with continuous effort during service hours until resolution or workaround is delivered.
 - **Severity 2 (Major):** 4-hour response, resolution within 3 working days.
 - **Severity 3 (Minor):** 8-hour response, resolution within 10 working days.
 - **Severity 4 (Trivial):** 1-day response, resolution within 30 working days.

Escalation and Communication

- If an incident is not resolved within the expected timeframe, it is escalated through management levels, with the customer kept informed at each stage.
- Customers can access support and updates via phone, email, an online portal, and regular service management reports.
- Regular service reviews and relationship management meetings ensure ongoing alignment and continuous improvement.

Additional Features

- The support service includes problem management (root cause analysis and prevention), release management (controlled deployment of changes), and service request handling (such as access control).
- Customers are expected to provide trained contacts for first- and second-line support, and to participate in service reviews and change management processes.

This approach ensures that service levels are transparent, measurable, and adaptable to the needs of each customer, with a strong focus on communication, accountability, and continuous improvement.

7. Business Continuity and Disaster Recovery Plan

OUR BUSINESS-CRITICAL INFORMATION AND SYSTEMS ARE BACKED UP DAILY

- Our well established and regularly audited Business Continuity and Disaster Recovery Plans mitigates against all possible risks. The CACI Business Continuity Plan is a living and continuously updated solution which exceeds the requirements of ISO27001 accreditation. It is reviewed formally on an annual basis by external auditors as part of our ISO27001 audit and is accessible to all staff, to keep in line with emerging risks. As such it has evolved over time as we have grown as a business and taken on a broader variety of work with a range of customer requirements. The Business Continuity Plan reflects the nature of the work we do and how we would be able continue delivering the work promised to our customers in the event of an emergency or major incident. The Business Continuity Plan also considers the ever-changing threats and current political climate to ensure that our response is up to date with the threats and pressures we maybe under as a business working in the Defence and Intelligence Industries.
- The Senior Leadership Team regularly review the plan to ensure that we are aware of any changing business factors for this to remain a compliant and realistic document.
- CACI's secure connections and encrypted back-up devices are checked monthly as part of our IT Security and Encryption Procedure. In addition, the encrypted back-ups are tested and sent off site at the end of each working day to a specialist storage contractor. CACI's office in Bristol requires several systems to be operational in order to deliver the services it provide to its customers; these are tested daily by a member of the CACI Bristol Technical Team and more rigorously tested monthly by the CACI IT team as part of their Security Incident Policy and Response Procedure. The Business Continuity Plan requires these systems to be operational and effective for staff to work remotely in case of an emergency or major incident. Agreements are also in place with partner organisation, so that staff working on secure projects have back-up locations to work from.
- CACI Information Intelligence Group have over 14 years of experience of providing mission-critical solutions and systems into HMG organisations.



NOTE: THIS DOCUMENT HAS BEEN CREATED AND SHARED FOR THE SOLE PURPOSE OF G-CLOUD BUYERS TO EVALUATE CACI AS A SUPPLIER. COPYING OR SHARING FOR ANY OTHER PURPOSE THAN THE AFOREMENTIONED IS PROHIBITED WITHOUT THE PRIOR CONSENT OF CACI LTD.

Thank you
