



# Crown Commercial Service

## G-Cloud 12 Call-Off Contract

This Call-Off Contract for the G-Cloud 12 Framework Agreement (RM1557.12) includes: Part A: Order Form ..... **Error! Bookmark not defined.**

Schedule 1: Services ..... 16

Schedule 2: Call-Off Contract charges ..... 16

Part B: Terms and conditions ..... 13

Schedule 3: Collaboration agreement ..... 32

Schedule 4: Alternative clauses ..... 44

Schedule 5: Guarantee ..... 49

Schedule 6: Glossary and interpretations ..... 57

Schedule 7: GDPR Information ..... 68

### Part A: Order Form

Buyers must use this template order form as the basis for all call-off contracts and must refrain from accepting a supplier's prepopulated version unless it has been carefully checked against template drafting.

Digital Marketplace service ID number	383089120611021
Call-Off Contract reference	C34149
Call-Off Contract title	Newborn Outcomes Support Contract

<b>Call-Off Contract description</b>	Annual maintenance contract for the Newborn Outcomes screening software solution that was developed by MDSAS and commissioned through DOS.
<b>Start date</b>	30/09/2021
<b>Expiry date</b>	29/09/2023
<b>Call-Off Contract value</b>	<p>£200,000 excluding VAT over 24 month period. Total support costs are £8,188.50 per quarter which equates to £65,508 over the 24 month period.</p> <p>Any development requirements will be called off subject to PHE internal approvals at the rate card set out below.</p>
<b>Charging method</b>	Invoice via BACS
<b>Purchase order number</b>	To Be Determined

This Order Form is issued under the G-Cloud 12 Framework Agreement (RM1557.12).

Buyers can use this Order Form to specify their G-Cloud service requirements when placing an Order.

The Order Form cannot be used to alter existing terms or add any extra terms that materially change the Deliverables offered by the Supplier and defined in the Application.

There are terms in the Call-Off Contract that may be defined in the Order Form. These are identified in the contract with square brackets.

<b>From the Buyer</b>	<div style="background-color: black; width: 200px; height: 15px; margin-bottom: 5px;"></div> Buyer's main address: 61 Colindale Avenue London NW9 5EQ
<b>To the Supplier</b>	Medical Data Solutions and Services Ltd (MDSAS) 0161 277 7917 5 Union Street, Manchester, M12 4JD
Together the 'Parties'	

## Principal contact details

### For the Buyer:

Title: National Programmes Lead (Antenatal and Newborn  
Screening Programmes)

Name:

Email:

Phone: 07917090164

**For the Supplier:**

Title: Director

Name: [REDACTED]

[REDACTED]

Email: [REDACTED]

Phone: [REDACTED]

**Call-Off Contract term**


<b>Start date</b>	This Call-Off Contract Starts on 30 September 2021 and is valid for 24 months
<b>Ending (termination)</b>	The notice period for the Supplier needed for Ending the Call-Off Contract is at least <b>90</b> Working Days from the date of written notice for undisputed sums or at least <b>30</b> days from the date of written notice for Ending without cause.
<b>Extension period</b>	<p>This Call-off Contract can be extended by the Buyer for [2] period(s) of up to 12 months each, by giving the Supplier (4) weeks written notice before its expiry.</p> <p>Extensions which extend the Term beyond 24 months are only permitted if the Supplier complies with the additional exit plan requirements at clauses 21.3 to 21.8.</p>

**Buyer contractual details**

This Order is for the G-Cloud Services outlined below. It is acknowledged by the Parties that the volume of the G-Cloud Services used by the Buyer may vary during this Call-Off Contract.

<b>G-Cloud lot</b>	This Call-Off Contract is for the provision of Services under: <b>Lot 2: Cloud software</b>
--------------------	--

<b>G-Cloud services required</b>	<p>The Services to be provided by the Supplier under the above Lot are listed in Framework Section 2 and outlined below:</p> <p>Service ID 383089120611021</p>
<b>Additional Services</b>	N/A
<b>Location</b>	The Services will be delivered remotely from the Supplier's premises and/or via remote working.
<b>Quality standards</b>	<p>The quality standards required for this Call-Off Contract are commensurate with Supplier G Cloud terms and CCS Standards. Suppliers are required to adhere to the Government's "Digital by Default" standards and those set out in Service ID 383089120611021</p>
<b>Technical standards:</b>	<p>The technical standards required for this Call-Off Contract are commensurate with Supplier G Cloud terms and CCS Standards. Suppliers are required to adhere to the Government's "Digital by Default" standards and those set out in Service ID 383089120611021.</p> <p>MDSAS is compliant with NHS Data Security and Protection toolkit which provides assurance on secure handling of NHS patient data. The Data Security and Protection Toolkit is an online self-assessment tool that allows organisations to measure their performance against the National Data Guardian's 10 data security standards.</p> <p>All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.</p>

<b>Service level agreement:</b>	<p>Service Requirements as set out in the attached document:</p>  <p>BOD 625 ECM 6702 Call-off Contract.pdf</p>
<b>Onboarding</b>	N/A
<b>Offboarding</b>	As set out in Service ID 383089120611021
<b>Collaboration agreement</b>	N/A
<b>Limit on Parties' liability</b>	<p>Subject to the provisions of Schedule 24 'Liability' of the Call-Off Agreement:</p> <p>The annual aggregate liability of either Party for all defaults resulting in direct loss of or damage to the property of the other Party (including technical infrastructure, assets, equipment or IPR but excluding any loss or damage to the Customer Data or Customer Personal Data) under or in connection with this Call- Off Agreement shall in no event exceed £1 million.</p> <p>The annual aggregate liability for all defaults resulting in direct loss, destruction, corruption, degradation or damage to the Customer Data or the Customer Personal Data or any copy of such Customer Data, caused by the Supplier's default under or in connection with this Call- Off Agreement shall in no event exceed £1 million of the Charges payable by the Customer to the Supplier during the Call- Off Agreement Period.</p> <p>The annual aggregate liability under this Call-Off Agreement of either Party for all defaults shall in no event exceed the greater of £100,000 or one hundred and twenty-five per cent (125%) per cent of the Charges payable by the Customer to the Supplier during the Call-Off Agreement Period</p>

<b>Insurance</b>	<p>The insurance(s) required will be:</p> <ul style="list-style-type: none"> <li>• A minimum insurance period of 6 years following the expiration or Ending of this Call-Off Contract</li> <li>• Professional indemnity insurance cover to be held by the Supplier and by any agent, Subcontractor or consultant involved in the supply of the G-Cloud Services. This professional indemnity insurance cover will have a minimum limit of indemnity of £1,000,000 for each individual claim or any higher limit the Buyer requires (and as required by Law)</li> <li>• Employers' liability insurance with a minimum limit of £5,000,000 or any higher minimum limit required by Law.</li> </ul>
<b>Force majeure</b>	<p>Neither Party shall be liable to the other Party for any delay in performing, or failure to perform, its obligations under this Call-Off Agreement to the extent that such delay or failure is a result of Force Majeure.</p> <p>Notwithstanding Clause 23, each Party shall use all reasonable endeavors to continue to perform its obligations under the Call-Off</p>
	<p>Agreement for the duration of such Force Majeure. However, if such Force Majeure prevents either Party from performing its material obligations under this Call-Off Agreement for a period in excess of one hundred and twenty (120) calendar days, either Party may terminate this Call-Off Agreement with immediate effect by notice in writing to the other Party.</p>

<b>Audit</b>	<p>The following Framework Agreement audit provisions will be incorporated under clause 2.1 of this Call-off Contract to enable the Buyer to carry out audits.</p> <ul style="list-style-type: none"> <li>• The Supplier will provide a completed self-audit certificate to CCS within 3 months of the expiry or Ending of this Framework Agreement.</li> <li>• The Supplier's record and accounts will be kept until the latest of the following dates:</li> <li>• 7 years after the date of Ending or expiry of this Framework Agreement</li> <li>• 7 years after the date of Ending or expiry of the last Call-Off Contract to expire or End</li> <li>• another date agreed between the Parties</li> <li>• CCS will use reasonable endeavours to ensure that the Audit does not unreasonably disrupt the Supplier, but the Supplier accepts that control over the conduct of Audits carried out by the auditors is outside of CCS's control.</li> <li>• Subject to any Confidentiality obligations, the Supplier will use reasonable endeavours to: <ul style="list-style-type: none"> <li>○ provide audit information without delay</li> <li>○ provide all audit information within scope and give auditors access to Supplier Staff</li> </ul> </li> </ul> <p>The Supplier will allow the representatives of CCS, Buyers receiving Services, the National Audit Office or auditors appointed by the Audit Commission access to the records, documents, and account information referred to in clause 7.7 (including at the Supplier's premises), as may be required by them, and subject to reasonable and appropriate confidentiality undertakings, to verify and review:</p> <ul style="list-style-type: none"> <li>○ the accuracy of Charges (and proposed or actual variations to them under this Framework Agreement)</li> <li>○ any books of accounts kept by the Supplier in connection with the provision of the G-Cloud Services for the purposes of auditing the Charges and Management Charges under the Framework Agreement and Call-Off Contract only</li> <li>○ the integrity, Confidentiality and security of the CCS Personal Data and the Buyer Data held or used by the Supplier</li> <li>○ any other aspect of the delivery of the Services including to review compliance with any legislation</li> <li>○ the accuracy and completeness of any MI delivered or required by the Framework Agreement</li> </ul>
--------------	--



	<ul style="list-style-type: none"> <li>○ any MI Reports or other records about the Supplier's performance of the Services and to verify that these reflect the Supplier's own internal reports and records</li> <li>○ the Buyers assets, including the Intellectual Property Rights, Equipment, facilities and maintenance, to ensure that the Buyers</li> <li>○ assets are secure, and that any asset register is up to date</li> </ul> <p>The Supplier will reimburse CCS its reasonable Audit costs if it reveals;</p> <ul style="list-style-type: none"> <li>• an underpayment by the Supplier to CCS in excess of 5% of the total Management Charge due in any monthly reporting and accounting Period</li> <li>• a Material Breach</li> </ul> <p>CCS can End this Framework Agreement under Section 5 (Ending and suspension of a supplier's appointment) for Material Breach if either event in clause 7.11 applies.</p>
<b>Buyer's responsibilities</b>	<ul style="list-style-type: none"> <li>• The Buyer is responsible for:</li> <li>• Co-operating with the supplier in all matters relating to the services</li> <li>• Complying with all dependencies and specific obligations on the Buyer set out in the agreement</li> <li>• The Buyer will ensure that it has a nominated representative available at all times for liaising with the Supplier</li> <li>• The Buyer will promptly provide the Supplier with such information as is requested by the Supplier from time to time</li> </ul>

	<ul style="list-style-type: none"> <li>• Provide timely access to the Buyers resources to enable the Supplier to provide the services as may be required from time to time</li> <li>•</li> </ul>
<b>Buyer's equipment</b>	The Buyer's equipment to be used with this Call-Off Contracts includes: N/A

## Supplier's information

<b>Subcontractors or partners</b>	The following list of the Supplier's Subcontractors or Partners:  N/A
-----------------------------------	---

## Call-Off Contract charges and payment

The Call-Off Contract charges and payment details are in the table below. See Schedule 2 for a full breakdown.

<b>Payment method</b>	The payment method for this Call-Off Contract is via BACS
<b>Payment profile</b>	The payment profile for this Call-Off Contract is payment against agreed milestones and deliverables, please refer to Schedule 2 of the Call-Off Contract.
<b>Invoice details</b>	The Supplier will issue electronic invoices against agreed milestone payments and deliverables. The Buyer will pay the Supplier within 30 days of receipt of a valid invoice.

<b>Who and where to send invoices to</b>	Invoices will be sent electronically to <a href="mailto:payables@phe.gov.uk">payables@phe.gov.uk</a>  *Paper invoices will be sent to: Public Health England Accounts Department Porton Site Manor Farm Road Porton Down
	Salisbury SP4 0JG  *Please note at the present time PHE are only accepting electronic invoices, should this change the Supplier will be advised.
<b>Invoice information required</b>	All invoices must include a purchase order with the Atamis Contract Reference Number, buyer copied into email, project reference required number and title.
<b>Invoice frequency</b>	Invoice will be sent to the Buyer following completion of agreed milestones (with frequency varying between individual services)
<b>Call-Off Contract value</b>	The total value of this Call-Off Contract is £200,000 Excluding VAT.
<b>Call-Off Contract charges</b>	The breakdown of the Charges is described in Schedule 2 of this Call-Off Contract.

### Additional Buyer terms

<b>Performance of the Service and Deliverables</b>	This Call-Off Contract will include the following Implementation Plan, exit and offboarding plans and milestones: The supplier must create an Exit Plan in accordance with paragraph 21 Exit Plan of the Call-Off.
<b>Guarantee</b>	N/A

<b>Warranties, representations</b>	<p>In addition to the incorporated Framework Agreement clause 4.1, the Supplier warrants representations: and represents to the Buyer that:</p> <ul style="list-style-type: none"> <li>• it has full capacity, authority and all necessary authorisations, consents, licenses and permissions, to enter into and perform its obligations under the Framework Agreement and each Call-Off Contract, including if a Supplier's processes need the consent of its Parent Company</li> </ul>
------------------------------------	--

	<ul style="list-style-type: none"> <li>• the Supplier or an authorised representative will sign the Framework Agreement and the Call-Off Contract</li> <li>• it has used and must continue to use all reasonable endeavors to prevent viruses and malware accessing systems owned by, under the control of, or used by CCS or any Buyer through its own access to these systems.</li> <li>• in entering into this Framework Agreement and any Call-Off Contract, it has not committed, will not commit or agree to commit a Prohibited Act</li> <li>• it will continue to pay all taxes due to HMRC and won't indulge in 'disguised employment' practices when delivering services under this Framework Agreement</li> <li>• at the Start Date, it has notified CCS in writing of any Tax Non-Compliance or any Tax Non- Compliance litigation it is involved in</li> <li>• it will perform all obligations under this Framework Agreement and any Call- Off Contract complying with all Laws</li> <li>• it will perform its obligations with all reasonable care, skill and diligence, according to Good Industry Practice.</li> <li>• on a Call-Off Start Date, all information, statements and representations in the Application are accurate and not misleading except if the Buyer has been notified in writing before signing the Call- Off Contract</li> <li>• The fact that any provision within this Framework Agreement is expressed as a warranty does not preclude any right of Ending CCS may have if the Supplier breaches that provision</li> </ul>
--	---

<b>Supplemental requirements in addition to the Call-Off terms</b>	<p>Supplemental requirements addition to call-off terms in the PHE will not be responsible in any way for the employment of staff involved in the IT support services and activities set-out in schedule 3 of this call-off contract.</p> <p>Please refer to Schedule 3.3 Deliverables for details.</p> <p>The Supplier must lodge a copy of the source code of the Newborn Outcomes System software with the Buyer's designated escrow account; NCC Group. The escrow account will be created, maintained and operated in the Buyer's name, and the Buyer will be the sole party authorised to grant escrow access.</p> <p>The Supplier grants the Buyer a non-exclusive, non-assignable, royalty-free licence to use the Supplier Background IPRs during the term of the Call-Off Contract for the sole purpose of enabling the Buyer to receive the Services and use any Deliverables.</p>
<b>Alternative clauses</b>	<p>In addition to the incorporated Framework Agreement clause 4, the Supplier warrants and represents to the Buyer that:</p> <ul style="list-style-type: none"> <li>• 4.11 The Parties do not intend the Framework Agreement to be used for provision of Services or off-payroll worker recruitment that is Inside 1R35.</li> <li>• 4.12 CCS may End this Framework Agreement under clause 5.1 for Material Breach if the Supplier is found to be delivering Services to a Buyer Inside 1R35.</li> </ul>
<b>Buyer specific amendments to/refinements of the Call-Off Contract terms</b>	<p>The contract may be altered at any time during the period of the contract, subject to Contract change notice (CCN) agreement signed off by both parties.</p>

<b>Public Services Network (PSN)</b>	<p>The Public Services Network (PSN) is the Governments secure network, if the G- Cloud Services are to be delivered over PSN this should be detailed here:</p> <p>Delivery of PSN Compliant Services</p> <p>If requested to do so by the Buyer, the Supplier shall ensure that the G-Cloud Services adhere to the conditions and obligations identified in the PSN Code of Practice at the Supplier's cost.</p> <p>If any PSN Services are Sub-Contracted by the Supplier, the Supplier must ensure that services have the relevant PSN compliance certification, which includes:</p> <ul style="list-style-type: none"> <li>• Buyer environments</li> <li>• Communications components</li> <li>• Compliant and certified</li> </ul> <p>Role of the PSN authority:</p> <ul style="list-style-type: none"> <li>• The Supplier will immediately disconnect its C-Cloud Services from the PSN if instructed to do so by the PSN Authority following an event affecting national security, or the security of the PSN. The Supplier agrees that the PSN Authority shall not be liable for any actions, damages, costs, and any other liabilities which may arise as a consequence.</li> <li>• This clause may be enforced by the PSN Authority, notwithstanding the fact that the PSN Authority is not a party to this Call-Off Contract.</li> <li>• Schedule 2, clause 12. Standards and quality</li> <li>• 14.1 The Supplier will comply with any standards in this Call-Off Contract, the Order Form and the Framework Agreement.</li> <li>• 14.2 The Supplier will deliver the Services in a way that enables the Buyer to comply with its obligations under the Technology Code of Practice, which is available at <a href="https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice">https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice</a></li> <li>• 14.3 If requested by the Buyer, the Supplier must, at its own cost, ensure that the G-Cloud Services comply with the requirements in the PSN Code of Practice.</li> <li>• 14.4 If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.</li> <li>• 14.5 The Supplier must immediately disconnect its G-Cloud Services from the PSN if the PSN Authority considers there is a risk to the PSN's security and the Supplier agrees that the Buyer and the PSN Authority will not be liable for any actions, damages, costs, and any other Supplier liabilities which may arise.</li> </ul>
--------------------------------------	--



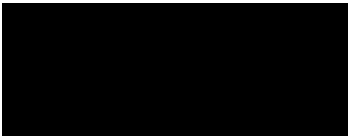
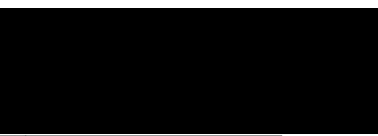
<b>Personal Data and Data Subjects</b>	Confirm whether Annex 1 (and Annex 2, if applicable) of Schedule 7 is being used: Annex 1, Annex 2;No
--	---

## 1. Formation of contract

- 1.1 By signing and returning this Order Form (Part A), the Supplier agrees to enter into a Call-Off Contract with the Buyer.
- 1.2 The Parties agree that they have read the Order Form (Part A) and the Call-Off Contract terms and by signing below agree to be bound by this Call-Off Contract.
- 1.3 This Call-Off Contract will be formed when the Buyer acknowledges receipt of the signed copy of the Order Form from the Supplier.
- 1.4 In cases of any ambiguity or conflict, the terms and conditions of the Call-Off Contract (Part B) and Order Form (Part A) will supersede those of the Supplier Terms and Conditions as per the order of precedence set out in clause 8.3 of the Framework Agreement.

## 2. Background to the agreement

- 2.1 The Supplier is a provider of G-Cloud Services and agreed to provide the Services under the terms of Framework Agreement number RM1557.12.
- 2.2 The Buyer provided an Order Form for Services to the Supplier.

<b>Signed</b>	Supplier	PHE, an Executive Agency of the Department of Health and Social Care
<b>Name</b>		
<b>Title</b>	Director of MDSAS	Director of Health Improvement Directorate
<b>Signature</b>		
<b>Date</b>	10/09/2021	07/09/2021

## Schedule 1: Services

The Supplier agrees to supply the G-Cloud Services and any G-Cloud Additional Services in accordance with the Call-Off Terms, including Supplier's own terms and conditions as identified in Framework Schedule 1 (G-Cloud Services) and incorporated into this Call-Off Agreement.

## Schedule 2: Call-Off Contract charges

For each individual Service, the applicable Call-Off Contract Charges (in accordance with the Supplier's Digital Marketplace pricing document) can't be amended during the term of the Call-Off Contract. The detailed Charges breakdown for the provision of Services during the Term will include:

Service NO.	Item	Service description
1	IT support desk (email and phone)	Ad hoc support questions, ranging from "how do I's?" to specific support on configuration, reporting, data manipulation, integrations etc.
2	Bug-fix development and implementation of PHE Newborn Outcomes system – front end / back end / API's	<p>Priority 1: System down – Escalated immediately to support staff with immediate action, continued until system restored.</p> <p>Priority 2: System bugs (with impact on operation) – response within three working hours of receiving call and resolution within 1 working day.</p> <p>Priority 3: System bugs with no serious effect on system performance or an enhancement request. For system bugs MDSAS will liaise with Product Owner.</p>
3	Maintaining user support system update documentation	Work closely with the Product Owner to update user guidance whenever there's a change to the system.
4	Central administration tasks e.g. maintenance of user lists, centres and documents	<p>Monitoring and support of staff in overseeing account maintenance. Account configuration, roles and centre creation</p> <p>Management of users, auditing and disabling accounts</p>



5	Domain name management N3 and Internet hosting on MDSAS Servers	Physical and virtual servers located at the data centre, N3 hosting and connectivity/BT line to access the servers
6	Implementation and support of system and database back-ups	<p>Creating and managing backup services for all PHE systems, including email system. Backup of web services are mirrored daily to secondary data centre. Additional SQL database is backed up nightly and stored electronically within the data centre.</p> <p>Configuring and delivering continued automated messaging for PHE and NHR users.</p>
7	Maintenance of network connectivity for sites	<p>Management of Server SSL certification</p> <p>System maintenance will be carried out with agreement of the Product Owner. Notification of agreed downtime will be specified in advance to users (usually a minimum of one weeks' notice will be provided).</p> <p>Unplanned outages will be processed as P1 support.</p>
8	Configuration, management and support of SQL Server database / reporting services	<p>Configuration and management of both the physical and virtual servers, including server operating systems, SQL servers and licences. Ongoing installation and management of server operating system and SQL server patches and service packs.</p> <p>Installation monitoring and upgrade of Microsoft Reporting Services (SSRS) and client-side components.</p> <p>Regular overview to ensure Reporting Services compatibility with other installed products remains intact.</p>
9	Gathering and dissemination of user update suggestions for further version releases	<p>MDSAS will collect user feedback and update suggestions and disseminate for further discussion with PHE. The Request for Change Process will be followed to agree further development work and version release.</p>

<b>10</b>	Account management and stakeholder liaison.	MDSAS will attend quarterly service review meetings to discuss service performance against the requirements set out within this SLA. MDSAS is required to produce evidence of service performance prior to the meetings. These meetings will take place via Skype or Webex
<b>12</b>	Disaster recovery contingency and test	planning and preparation for the outage
<b>13</b>	Quarterly stats	creating of quarterly performance review stats
<b>17</b>	Account management and stakeholder liaison.	MDSAS may attend three user group meetings every year to gain user feedback, discuss and test requests for change and development of the system. These will be face-to-face meetings, usually held in London. Travel will be organised and paid for by PHE in line with PHE expense policy.
<b>18</b>	Penetration testing	MDSAS will undertake penetration testing annually in line with ICO security guidance <a href="https://ico.org.uk/for-organisations/guidetodata-protection/guide-to-the-generaldata-protection-regulation-gdpr/security/">https://ico.org.uk/for-organisations/guidetodata-protection/guide-to-the-generaldata-protection-regulation-gdpr/security/</a>

Total Annual Cost of £32,754 excluding VAT.

#### Development work

Cost of development of new functionality will be based on a time and materials basis. To cover development, documentation, testing & QA, engagement at scoping, user feedback, project management and executive overview, this will be at a rate of £803 excluding VAT per development day i.e. charges will only be incurred for the number of development days.

## **1: Service Levels:**

### **1.1 Service Levels for the Help Desk**

**The Supplier shall meet or exceed the following Service Levels:**

Definition	Service Level
Availability of the Help Desk	Core Hours. (Mon - Friday 09. 00 -17.00 hours excluding bank holidays)
Response Time (measured during Core Hours)	<p>A central help desk is available throughout the working day via email and phone</p> <p>Switch to voicemail Add in when the call switches to voicemail (timeframe). Is it available out of hours? (expect that all calls are held in a queue or go to voicemail?)where the central call desk and support team are not available.</p> <p>A help desk analyst will check all voicemails every 30 minutes during Core Hours.</p> <p>Emails are constantly reviewed and prioritised as they arrive.</p>
Service Credits	No Service Credits apply to the above Service Levels.

### **1.2 Priority Levels for Core System**

Incident priority levels are defined as follows:

Incident priority levels are defined as follows:

Definition	Measure	Measurement period	Service Credits
Availability of the Core System	97.0%	Quarterly	Yes (in accordance with section 9 & 10)

Priority 1 incident Response	Within 1 Core Hour	Quarterly	No
Priority 2 incident Response	Within 3 Core Hours	Quarterly	No
Priority 3 incident Response	Within 10 Core Hours	Quarterly	No
Definition	Measure	Measurement period	Service Credits
Priority 1 incident fix	Resolution within 6 Core Working Hours	Quarterly	Yes
Priority 2 incident fix	Resolution within 1 Working Day	Quarterly	Yes
Priority 3 incident fix	85% Resolved within 3 Working Days.	Quarterly	Yes
Priority 4 incidents fix (bugs)	75% Resolved within 90 days 95% Resolved within 180 days	Rolling 90 days Rolling 180 days	No No
Priority 5 incidents (changes)	100% costed within 90 days	Rolling 90 days	No

Yearly P1	6 or less a Year	Yearly	No
Priority 1 & 2 incidents	In Year two less than 4 per Month	Yearly	No
Time taken to log on to application (measured from the point at which the user enters the correct password and ending when the initial menu screen appears)	99.9% < 5 seconds	Quarterly	No
Search and retrieval of individual record (measured from the points at which the search key is depressed to the point at which the requested record is returned)	99.9% < 5 seconds	Quarterly	No

### 1.3 Service Levels for the Core System

The Supplier shall meet or exceed the following Service Levels:

See appendix 1 for **Priority Levels for Core System**

Definition	Measure	Measurement period	Service Credits
Availability of the Core System	97.0%	Quarterly	Yes (in accordance with section 9 & 10)
Priority 1 incident Response	Within 1 Core Hour	Quarterly	No

Priority 2 incident Response	Within 3 Core Hours	Quarterly	No
Priority 3 incident Response	Within 10 Core Hours	Quarterly	No
Priority 1 incident fix	Resolution within 6 Core Hours1 Working Day	Quarterly	Yes (in accordance with section 9 & 10)
Priority 2 incident fix	Resolution within 1 Working Day	Quarterly	Yes (in accordance with section 9 & 10)
Priority 3 incident fix	85% Resolved within 3 Working Days.	Quarterly	Yes (in accordance with section 9 & 10) this Appendix)
Priority 4 incidents fix (bugs)	75% Resolved within 90 days	Rolling 90 days	No
	95% Resolved within 180 days	Rolling 180 days	No
Priority 5 incidents (changes)	100% costed within 90 days	Rolling 90 days	No
Yearly P1	6 or less a Year	Yearly	No
Priority 1 & 2	In Year two less	Yearly	No
Definition	Measure	Measurement period	Service Credits
incidents	than 4 per Month		
Time taken to log on to application (measured from the point at which the user enters the correct password and ending when the initial menu screen appears)	99.9% < 5 seconds	Quarterly	No

Search and retrieval of individual record (measured from the points at which the search key is depressed to the point at which the requested record is returned)	99.9% < 5 seconds	Quarterly	No

#### *1.4 Service Levels for the Disaster Recovery ("DR") Service*

**The Supplier shall meet or exceed the following Service Levels:**

Description	Measurement
Response Time	From reporting or identification of issue to invocation of Disaster Recovery Plan: 2 hours.
Recovery	Solution to be fully operational within 1 Working Day of invocation of Disaster Recovery Plan.
	Recovery of all data, if possible, prior to invocation of Disaster Recovery Plan within 5 Working Days of invocation.
Service Credits	Measurement of Service Levels shall be suspended once the Disaster Recovery Plan is invoked, and shall resume from the time at which the Parties agree that the Disaster Recovery Plan has been completed, or at the end of 5 Working Days following invocation (whichever is earlier).
Annual Test	A test will be undertaken annually to simulate a working Core System at the disaster recovery site. This will be achieved by replicating the Core Systems at the disaster recovery site and demonstrating the active running of each of the components.

## 2: Performance Monitoring

### 2.1 Service Reviews

Within 10 Working Days of the end of each quarter the Supplier shall provide a Performance Monitoring Report to the Buyer's IT Contract Manager.

The Performance Monitoring Report shall be in the form of a MS Word document and shall contain, as a minimum, the following information in respect of the quarter just ended:

A RAG rated table summarising performance of Service Levels detailing the levels of performance specified by this Contract and actual performance over the previous twelve (12) month period;

For each Service Level, the actual performance achieved over the quarter, and that achieved over the previous twelve (12) months;

A summary of all failures to meet Service Levels that occurred during the quarter;

The level of each failure to meet Service Levels which occurred;

Which service failures remain outstanding and progress in resolving them;

For any Priority 1 incidents occurring in the quarter, the cause of the fault and any action being taken to reduce the likelihood of recurrence;

For any repeat failures, actions taken to resolve the underlying cause and prevent recurrence;

The Service Credits to be applied in respect of that quarter indicating the service failure(s) to which the Service Credits relate;

Relevant particulars of any aspects of the performance by the Supplier which fail to meet the requirements of this Contract; and

Unless otherwise agreed, the parties shall attend Performance Review Meetings on a quarterly basis via teleconference or WebEx. The Performance Review Meetings will be the forum for the review by the Supplier and the Buyer of the Performance Monitoring Reports and Reporting Summaries (where relevant). The Performance Review Meetings shall (unless otherwise agreed):

Take place within two (2) weeks of the Performance Monitoring Report being issued by the Supplier;

have actions recorded by the Supplier

### 2.2 Exclusions

If any issues occur which are out of the control of the Supplier then these issues are excluded from all performance metrics and penalties.

If performance issues are identified between quarterly meetings and performance has dropped below the thresholds specified above, the Buyer has the right to call additional performance meetings and request



supporting information and documentation to agree a performance action plan and to verify the required level of performance has been restored.

### **3 Availability**

Whilst the Solution is required to be Available 24/7 365 days (or 366 in a leap year) a year, Service Levels shall be measured during Core Hours only and Service Credits shall accrue only in relation to failure to achieve the applicable Availability Service Levels in the server and software infrastructure designed for production use. In addition, the Supplier shall report against the Availability Service Levels in relation to each of the training environment and test environment.

**Availability will be measured Quarterly by reference to the following formula:**

$$(A - B) / A * 100 = \text{Availability}$$

A = the total number of minutes in a Quarter during Core Hours less the number of minutes of Scheduled Down Time and Emergency Downtime for maintenance.

B = the number of minutes during Quarter when the relevant system is "Unavailable". For these purposes (i) the said number of minutes shall accrue from the time that relevant component of the Core System becomes Unavailable up until the time that the relevant component(s) become Available again, and according to whether the Availability of the Core System and (ii) the number of minutes during which the relevant system is Unavailable due to any Exceptions shall be disregarded. If more than one relevant component is Unavailable during a period of time, the minutes of Unavailability shall only accrue once during such overlapping period. For example, if the following components of the Core System were Unavailable one morning during the times set out in the table below, the number of minutes of Unavailability for the purposes of the Availability formula and calculation of Services Credits would be 60 (sixty):

<b>Core System component</b>	<b>Period of Unavailability</b>
Correspondence module	09:00 – 09:30
Search	09:15 – 09:45
User interface	09.20 – 10.00

In addition, when measuring Availability of the Core System any period of time during which the Help Desk is Unavailable shall (subject to the provisions above regarding overlapping periods of Unavailability) be aggregated with the period of time during which the Core System is Unavailable.

For these purposes each component shall mean a separate logical entity of the Core System which shall deliver the function and performance specified in this Contract in relation to it.

The following Service Credits shall apply where Service Levels are not met in respect Core System Availability:

*Table 1*

Core Hours Core System Unavailable in Quarter	Years 1,2
	SCT outcomes Solution
≤ 12	Nil
> 12 and ≤ 24	£157.25
> 24 and ≤ 36	£314.50
> 36 and ≤ 48	£471.75
> 48 and ≤ 60	£629
> 60	£786.25

#### **4: Service Credits and Service Failure points**

4.1 Subject to this paragraph 4.1 and paragraphs 4.2 – 4.4 below, Service Credits shall be the Buyer's sole and exclusive financial remedy in the event that the Supplier fails to achieve the Availability Service Level due to its default unless:

- (a) any failure to meet the Service Levels (either on an individual basis or in aggregate) constitutes a failure beyond that for which the Service Credits have been set; or
- (b) the Buyer is otherwise entitled to terminate this Contract; or
- (c) the failure to perform the Services in accordance with the Service Levels has arisen due to theft, gross negligence, fraud, fraudulent misrepresentation or wilful default; or
- (d) the failure to perform the Services in accordance with the Service Levels results in a material and irredeemable corruption or loss of data,

in which case the Buyer may obtain such other remedies as may be available to it, either under this Contract or otherwise at law or in equity, including the right to terminate this Contract.

4.2 If the Availability of the Core System falls below 95% of Core Hours, in aggregate, in any Quarter, the Supplier shall immediately escalate the matter to its Board and shall, within five (5) Working Days of the same, submit a written remedial plan to the Buyer identifying the corrective actions that the Supplier will take to improve the Availability performance so that it meets the Availability Service Level. Within 5 Working Day of receipt of the remedial plan, the Buyer shall either review and approve it or shall reject the same. If the Buyer rejects the remedial plan, the Supplier shall have a further 5 Working Days within which to resubmit the remedial plan with such changes as are required and the Buyer shall have five (5) Working Days from receipt of the same to review the re-submitted remedial plan. The parties also acknowledge that in relation to the New Solution Software as a whole

(both the Core System), a provision similar to that set out in this paragraph 10.2 shall apply, subject to the parties agreeing in writing the applicable threshold (percentage of Core Hours Availability) and any other relevant factors to be taken into account in relation to the obligation to submit a remedial plan.

4.3 Without prejudice to any other rights or remedies of the Buyer in the event that:

4.3.1.1 the Supplier fails to meet the Availability times in accordance with any remedial plan approved under paragraph 10.2 above; or

4.3.1.2 the Buyer rejects the remedial plan submitted under paragraph 10.2 for a second time and the Supplier does not within 30 days of the rejection of the remedial plan meet the said Service Level; or

4.3.1.3 the Supplier presents a remedial plan pursuant to paragraph 10.2 and this is rejected on a second occasion by the Buyer, and within the previous 24 month period a remedial plan has been rejected on a second occasion and following rejection of such remedial plan (presented during the said previous 24 month period) the Supplier has subsequently met the relevant Service Level within the 30 day period referred to above at paragraph (b);

then the Buyer shall be immediately entitled to terminate the Contract.

4.4 The Buyer shall not unreasonably withhold or delay its approval of any remedial plan produced by the Supplier in accordance with paragraphs 4.2 - 4.4.

## **5 Response Times Service Levels**

5.1 The Supplier and the Buyer have agreed the Response Time Service Levels set out in Section 7

5.2 In any Quarter failure to achieve the Response times Service Levels as defined in section 7 & 8 will result in the Supplier producing a remedial plan within 5 Working Days to address the Response time issues.

## **6 Resolution Time Service Levels and associated Service Credit Regime**

6.1 Failure to achieve the Resolution times Service Levels will result in the allocation of Service Failure Points (“SFPs”) as detailed in Table 2 below.

6.2 Subject to paragraph 6 and 5.2 below, the Service Credit to be applied as a result of the accumulation of allocated SFPs is set out in Table 2 below.

6.3 Subject to this paragraph 3.3 and paragraphs 3.4 and 4 below, Service Credits shall be the Buyer’s sole and exclusive financial remedy in the event that the Supplier fails to achieve the Resolution times set out in this Appendix 3 unless:

6.3.1 any failure to meet the Service Levels (either on an individual basis or in aggregate) constitutes a failure beyond that for which the Service Credits have been set; or

6.3.2 the Buyer is otherwise entitled to terminate this Contract; or

6.3.3 the failure to perform the Services in accordance with the Service Levels has arisen due to theft, gross negligence, fraud, fraudulent misrepresentation or wilful default; or

6.3.4 the failure to perform the Services in accordance with the Service Levels results in a material and irredeemable corruption or loss of data,

in which case the Buyer may obtain such other remedies as may be available to it, either under this Contract or otherwise at law or in equity, including the right to terminate this Contract

*Table 2*

Priority Level	Maximum Resolution Time	No. of allocated Service Failure Points for failure to resolve in the timescales
1	< 4 Core Hours	Nil
	< 6 Core Hours	6
	<1 Working Day	12
	<3 Working Days	18
	> 5 Working Days	50
2	< 1 Working Day	Nil
	<1 ½ Working Days	4
	<2 Working Days	6
	<7 Working Days	8
	> 7 Working Days	24
3	> 7 Working Days	2

Service Credit for Total Accrued SFPs		
Total Accrued SFPs per Quarter	Service credit per Quarter	
	SCT Newborn outcomes system	
≤ 20	Nil	
21 – 40	£157.25	
41 – 60	£314.50	

61 – 80	£471.75
81 – 100	£629
> 100	£786.25

10.1 If the total accrued SFPs for failure to resolve issues within agreed timescales reaches or exceeds 51 in any Quarter, then the Supplier must submit a plan to address the root cause of the problem and instigate any recommendations within thirty (30) Working Days of the end of the Quarter.

## Appendix 1 Priority Levels for Core System

Incident priority levels are defined as follows:

Incident Priority Level	Definition
-------------------------------	------------

<b>Priority 1</b>	<p>Any incident shall be categorised as Priority 1 where an immediate action is required because a significant part of the service is unavailable, resulting in users being unable to perform their duties or a clinical incident arises, in each case which meets the applicable criteria below.</p> <p>A service failure which, in the reasonable opinion of the Buyer and or Service User:</p> <ul style="list-style-type: none"> <li>• constitutes a loss of the Core System which prevents more than 45% of end users or Service Users from working; or</li> <li>• has a critical impact on the activities of the Buyer or Service User; or</li> <li>• causes significant financial loss and/or disruption to the Buyer or Service User; or</li> <li>• results in any material loss or corruption of Buyer or Service User data; or</li> <li>• presents a clinical safety issue; or</li> <li>• prevents an end user or Service User from logging an incident with the Help Desk.</li> </ul> <p>Non-exhaustive list of examples:</p> <ul style="list-style-type: none"> <li>• loss of access or function to 45% or more of the users base to any core component of the Core System, e.g. single sign on, patient searches/Patient lists, ability to access a site or facility, printing documents or generating reports and loss of data feed from labs;</li> <li>• performance rendering the Core System unusable;</li> <li>• where 5 or more Service Users report the Core System is: <ul style="list-style-type: none"> <li>○ presenting recorded or calculated clinical data incorrectly</li> </ul> </li> </ul>
<b>Incident Priority Level</b>	<b>Definition</b>
	<p>leading to an incorrect screening pathway decision for the patient (e.g. clear outcome where the outcome should be no clear)</p> <ul style="list-style-type: none"> <li>• security is compromised: the Core System contains a bug that enables users to bypass security; the Core System is not maintaining legitimate relationships</li> </ul>

## Appendix 2:

Breakdown of software and software licence terms and hardware components:

### Supplier to input their response

	Software	Supplier (if affiliate of the SERVICE PROVIDER )	High level description	To be deposited in escrow	Restrictions	Other	Core Systems or Noncore System – please specify
1	Newborn Outcomes System	N/A	The Newborn Outcomes System	Yes	None	N/A	Core
2	NHR Portal	N/A	Ability to access the Newborn Outcomes System through the National Haemoglobinopathy Registry	No	Restricted to Newborn Outcomes portal	N/A	Core
3	MDSAS Hardware Infrastructure	N/A	DELL Poweredge Servers	No	2xE52699v3 16x16GB 4x600GB RPSU 3	N/A	Core

## Appendix 3:

### Non-Functional Requirements:

Provide secure and controlled access to patient data:	The Newborn Outcomes system is hosted on secure servers within the Leigh NHS data centre. The system is only accessible from within the NHS N3 network.
Maintain an appropriate level of security and anonymity, including the use of role based access rights to ensure that access to patient records are restricted to personnel who are involved in the care of that patient.	Authentication is controlled through username and password. Role-based access control is employed within the system to ensure users only have access to functions / resources they are authorised to do so. For example Treatment Centres only have access to patient information about patients in their care.
Track access to patient records in order to provide a forensic capability in case of a breach of data access rules	The system records
Comply with the requirements of the Information Governance	MDSAS hold IG toolkit level 2 or above on all requirements <a href="https://www.igt.hscic.gov.uk/assessmentreportcriteria.aspx?tk=431706476974089&amp;Inv=3&amp;cb=044431b2-1a43-438b-a425-8b1040588741&amp;rpprms=26442~False~8HM29~261~False~False~False~False~False~">https://www.igt.hscic.gov.uk/assessmentreportcriteria.aspx?tk=431706476974089&amp;Inv=3&amp;cb=044431b2-1a43-438b-a425-8b1040588741&amp;rpprms=26442~False~8HM29~261~False~False~False~False~False~</a>
Statement of Compliance (IGSOC)	<b>Information Governance Assurance Statement</b>
	Information Governance Assurance Statement for Organisations that use, or plan to use NHS Digital Services  Version 4, 10/06/2014



	<ol style="list-style-type: none"> <li>1. All organisations that have either direct or indirect access to NHS Digital services<sup>1</sup>, including N3, must complete an annual Information Governance Toolkit Assessment and agree to the following additional terms and conditions. Where the Information Governance Toolkit requirements are not met to an appropriate standard (minimum level 2), an action plan for making the necessary improvements must be agreed with the NHS Digital External Information Governance team or with an alternative body designated by the Department of Health (e.g. a commissioning organisation).</li> <li>2. All organisations providing indirect access<sup>2</sup> to NHS Digital services for other organisations (approved N3 link recipients), are required to provide the Department of Health, on request, with details of all organisations that have been permitted access, the business justification and the controls applied, and must maintain a local log of organisations to which they have allowed access to N3. This log should be reviewed regularly by the organisation and unnecessary access rights removed. The Department of Health or an alternative body designated by the Department of Health may request sight of these logs in order to facilitate or aid audit or investigations.</li> <li>3. The approved N3 link recipient is responsible for their compliance with IG policies and procedures and may request authorisation by the Department of Health to monitor and enforce the compliance and conduct of subsidiary connected organisations and suppliers to ensure that all key information governance requirements are met.</li> <li>4. The use of NHS Digital Services should be conducted to support NHS business activities that contribute to the care of patients. Usage of individual services must be conducted inline with those individual services requirements and acceptable use policies. The use of NHS Digital provided infrastructure or services for unauthorised advertising or other non-healthcare related activity is expressly forbidden.</li> <li>5. All threats or security events affecting or potentially affecting the security of NHS Digital</li> </ol>
--	---

	<p>provided infrastructure or services must be immediately reported via the NHS Digital incident reporting arrangements or via local security incident procedures where applicable.</p> <p>6. All infrastructure and connections to other systems and networks which are not covered by an approved Information Governance Toolkit Assessment and agreement to this IG Assurance Statement must be segregated or isolated from IGT covered infrastructure and connections such that IGT covered infrastructure and connections, or NHS Digital Services are not put at risk. A Logical Connection Architecture diagram must be maintained by network managers in accordance with NHS Digital guidance and must be provided for Department of Health review on request.</p> <p>7. Organisations with access to NHS Digital Services shall ensure that they meet the requirements of the Department of Health policy on person identifiable data leaving England, or being viewed from overseas. A copy of the Information Governance Offshore Support Requirements applicable to those accessing NHS Digital Services is available on request or can be downloaded from <a href="http://systems.hscic.gov.uk/infogov/igsoc/links/index.html">http://systems.hscic.gov.uk/infogov/igsoc/links/index.html</a>. The agreement of the Department to this limited support or exceptionally to more extensive processing must be explicitly obtained.</p> <p>8. Where another network is connected to N3, only services that have been previously considered and approved by the Department of Health as appropriate for that network are permissible. Requests for new or changed services must be provided to the Department for consideration.</p> <p>9. Organisations may not create or establish any onward connections to the N3 Network or NHS Digital provided services from systems and networks which are not covered by an approved Information Governance Toolkit Assessment and agreement to this IG Assurance Statement.</p> <p>10. The approved organisation shall allow the Department of Health, or its representatives, to carry out ad-hoc on-site audits, and to review any/all evidence that supports the Information Governance Toolkit Assessment, as necessary to confirm compliance with these terms and</p>
--	--

	<p>conditions and with the standards set out in the Information Governance Toolkit.</p> <p>Information Governance Assurance Statement</p> <p>I confirm that I have read, understood and agree to comply with the additional terms and conditions that apply to organisations that have access to NHS Digital services and acknowledge that failure to maintain compliance may result in the withdrawal of NHS Digital services.</p> <p><sup>1</sup> NHS Digital Services include the N3 network and other applications or services provided by NHS Digital, e.g. the NHS Spine Service, NHSmail, Choose and Book (and in future the NHS e-Referral Service).</p> <p><sup>2</sup> Access to the N3 network or NHS Digital Services via another organisation or gateway</p> <p>Statement accepted by <b>Paul Kane (pauljkane)</b> at <b>29/06/2018 12:56</b> on behalf of <b>Medical Data Solutions and Services</b> against IG Toolkit Requirements Version <b>14.1</b></p>
Maintain integrity of data	Various - All data will be retained by MDSAS (the data processor) in strict accordance with UK regulations and PHE (the data controller) instructions.
No loss of data	The servers are mirrored across two independent data centres, providing continuous data availability and avoiding downtime. Full data backups are performed nightly. Nightly data backups are currently archived after 1 year, whereby a monthly backup is retained indefinitely.
No loss of consistency in reporting	MDSAS and NCARDRS have agreed frequency and format of reports

## Appendix 4:

### Data Flows and Data Sharing

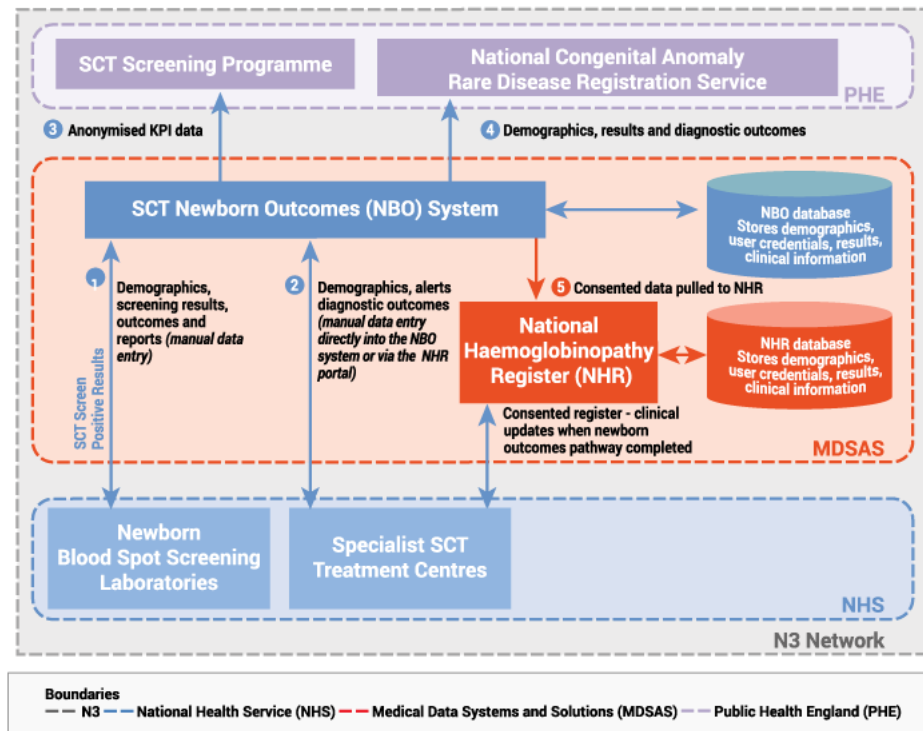
The newborn outcomes system automates referral of infants that screen positive for sickle cell disease and thalassaemia and supports the collection and reporting of data. It replaces existing data flows used to support the newborn outcomes project previously run by KCL and currently held by NCARDRS, PHE and includes the same data set.

The referral is created in the screening laboratory and shared with clinical centre(s) depending on local pathway. Data is added to the record by clinical teams.

Removing the need for clinicians to enter the same data twice (e.g. demographics, screening results, etc.) is one of the key requirements for the project. To enable integration with the NHR people who already have a user account on the NHR, will access the SCT Newborn Outcomes system through an interface in the NHR rather than logging in to a separate system.

The interface in the NHR matches the main SCT Newborn Outcomes System, and is provided as a 'view' onto the system for NHR users.

#### Data flows:



Screening is a direct care service, newborn blood spot screening is recommended but it is not compulsory. Parental agreement is needed for children to be screened and this permission can be verbal; there is no need to separately obtain parental agreement for data to be used for QA and programme management purposes.

PHE is party to the S7A agreement with NHS England that covers the provision of screening services by the NHS.

The lawful basis for PHE to process personal data in the Newborn Outcomes System (**points 1 and 2**) is provided by General Data Protection Regulations (GDPR):

- article 6(1)(e) - for the performance of a task carried out in the public interest or in the exercise of official authority and;
- 9(2)(i) - for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices.

Data is shared with NCARDS (point 4) who have permission from the National Information Governance Board under section 251 the NHS Health Act 2006 and the authority of the Health Service (Control of Patient Information) Regulations 2002, to collect patient-identifiable data without the need for individual informed consent for the purposes of congenital anomaly and rare disease registration. The system will automatically generate and transfer specific data to NCARDS on a weekly basis.

The National Haemoglobinopathy Register (NHR) is commissioned by NHS England. It is a database of patients with haemoglobinopathies living in the UK. Data is collected from clinicians in Haemoglobinopathy Centres. The central aim of the registry is to improve patient care. National Haemoglobinopathy Register (NHR) users access the PHE system from a single login. This interface is provided as a convenience function to allow NHR users to view and use the SCT Newborn Outcomes System without a separate login. It does not affect the process or data collected. All data is held in the Newborn Outcomes System. The NHR is a consented register and no data crosses into the NHR until consent has been explicitly recorded (**point 5**). The Newborn Outcomes system collects only a minimum data set additional data items recorded on the NHR are not shared back.

De-personalised KPI data reports (**point 3**), are returned to the NHS SCT screening programme.

Information about what personally identifiable information is used by the screening programmes and why is provided in “Screening tests for you and your baby”, a booklet issued to all pregnant women in England with more detailed information on [Gov.UK](https://www.gov.uk). This includes the parent’s right to opt out of their data being held in NCARDRS under Section 251 approval.

More information on the [NHR](#) can be found on their website and includes [a patient information leaflet](#).

## Data items and purpose of sharing

Data item	Purpose
Name of newborn screening (NBS) laboratory (from login)	To identify NBS laboratory responsible for testing the sample and making the referral
Contact email address (from login)	As above

Data item	Purpose
Type of centre	To distinguish between nursing and medical centre according to local pathway
Name of centre	To identify correct centre for referral
Contact email address	To notify new referral by email in addition to insystem
Name of nurse/counsellor/doctor	To identify healthcare professional(s) who will receive the referral and for audit purposes
Unique laboratory reference/card serial number	To provide linkage back to the NBS card
NHS number	To identify the baby across NHS care settings

Baby/child's family name / surname at birth	(Surname at birth) to identify the baby
Baby/child's registered surname (if different)	Surname may change between birth and 42 days (the legal requirement to register the birth)
Baby/child's first name	(First name) to identify the baby
Sex	To identify the baby and to analyse data for difference by gender
Date of birth	To identify the baby and measure performance against KPIs
Gestation of baby at birth	Necessary to interpret baby's screening results
Baby's address line 1	To identify and track baby
Baby's address line 2	As above
Baby's address line 3	As above
Baby's postcode	As above
Ethnic origin	To monitor the disease prevalence by ethnicity and for equality monitoring
Has the baby or child had a blood transfusion?	Necessary to interpret baby's screening results
GP name	To identify and track baby
GP practice code	To identify and track baby
Date of newborn screening test result	To identify the baby and measure performance against KPIs

<b>Data item</b>	<b>Purpose</b>
Newborn screening result	Communicate which condition is suspected
Any other comments on the result	Additional information to clarify result
Mother's NHS number	To improve identification of babies, needed for dataset linkage and quality assurance of linked programme

Mother's surname	As above
Mother's forename	As above
Mother's Hb carrier/affected state	Required to confirm baby's diagnosis in some cases and to evaluate antenatal and newborn linked programme and quality assurance
Father's Hb carrier/affected state	Required to confirm baby's diagnosis in some cases and to evaluate antenatal and newborn linked programme and quality assurance
Prenatal diagnosis (PND) offered/accepted/declined	Evaluate antenatal and newborn linked programme and quality assurance
PND result	Evaluate antenatal and newborn linked programme and quality assurance
Baby/child's hospital number	Unique identifier within an organisation setting
Date NBS results received	To identify the baby and measure performance against KPIs
Date screening result reported to parents	To measure performance against KPIs
Date baby/child attended the haemoglobinopathy medical centre	Confirmation of handover to treatment services and to measure performance against KPIs
Confirmed screening results	Evaluate antenatal and newborn linked programme and quality assurance
Confirmed diagnosis	Evaluate antenatal and newborn linked programme and quality assurance
<b>Data item</b>	<b>Purpose</b>
Date penicillin offered / prescribed/declined (SCD only)	Evaluate antenatal and newborn linked programme and quality assurance
Clinical comments	Additional information to clarify result

Date of death	Evaluate antenatal and newborn linked programme and quality assurance
Cause of death	Evaluate antenatal and newborn linked programme and quality assurance To determine if death can be ascribed to sickle cell disease or thalassaemia

### **Data retention:**

Based on current legal requirements, professional best practice and user needs, data will be retained until the 25<sup>th</sup> birthday<sup>1</sup>.

<https://digital.nhs.uk/data-and-information/looking-after-information/data-security-andinformationgovernance/codes-of-practice-for-handling-information-in-health-andcare/records-management-code-ofpractice-for-health-and-social-care-2016>

## **Appendix 4:**

### **Data Flows and Data Sharing**

The newborn outcomes system automates referral of infants that screen positive for sickle cell disease and thalassaemia and supports the collection and reporting of data. It replaces existing data flows used to support the newborn outcomes project previously run by KCL and currently held by NCARDRS, PHE and includes the same data set.

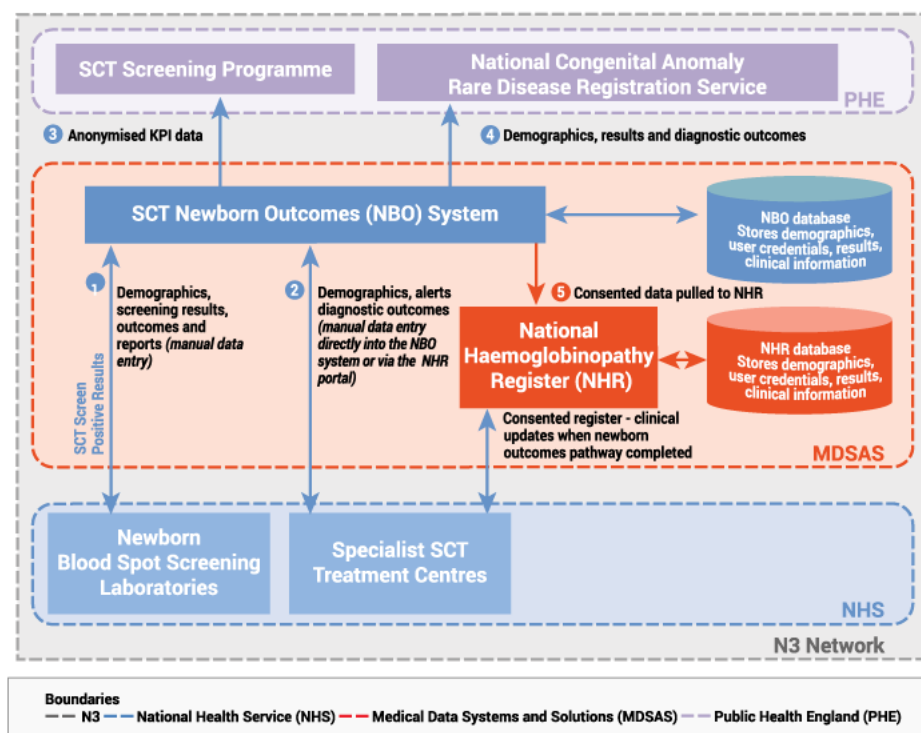
The referral is created in the screening laboratory and shared with clinical centre(s) depending on local pathway. Data is added to the record by clinical teams.

Removing the need for clinicians to enter the same data twice (e.g. demographics, screening results, etc.) is one of the key requirements for the project. To enable integration with the NHR people who already have a user account on the NHR, will access the SCT Newborn Outcomes system through an interface in the NHR rather than logging in to a separate system.

The interface in the NHR matches the main SCT Newborn Outcomes System, and is provided as a 'view' onto the system for NHR users.

### **Data flows:**





Screening is a direct care service, newborn blood spot screening is recommended but it is not compulsory. Parental agreement is needed for children to be screened and this permission can be verbal; there is no need to separately obtain parental agreement for data to be used for QA and programme management purposes.

PHE is party to the [S7A agreement](#) with NHS England that covers the provision of screening services by the NHS.

The lawful basis for PHE to process personal data in the Newborn Outcomes System (**points 1 and 2**) is provided by General Data Protection Regulations (GDPR):

- article 6(1)(e) - for the performance of a task carried out in the public interest or in the exercise of official authority and;
- 9(2)(i) - for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices.

Data is shared with NCARDRS (**point 4**) who have permission from the National Information Governance Board under section 251 the NHS Health Act 2006 and the authority of the Health Service (Control of Patient Information) Regulations 2002, to collect patient-identifiable data without the need for individual informed consent for the purposes of congenital anomaly and rare disease registration. The system will automatically generate and transfer specific data to NCARDRS on a weekly basis.

The National Haemoglobinopathy Register (NHR) is commissioned by NHS England. It is a database of patients with haemoglobinopathies living in the UK. Data is collected from clinicians in Haemoglobinopathy Centres. The central aim of the registry is to improve patient care. National Haemoglobinopathy Register (NHR) users access the PHE system from a single login. This interface is provided as a convenience function to allow NHR users to view and use the SCT

Newborn Outcomes System without a separate login. It does not affect the process or data collected. All data is held in the Newborn Outcomes System. The NHR is a consented register and no data crosses into the NHR until consent has been explicitly recorded (**point 5**). The Newborn Outcomes system collects only a minimum data set additional data items recorded on the NHR are not shared back.

De-personalised KPI data reports (**point 3**), are returned to the NHS SCT screening programme.

Information about what personally identifiable information is used by the screening programmes and why is provided in “Screening tests for you and your baby”, a booklet issued to all pregnant women in England with more detailed information on

Gov.UK. This includes the parent’s right to opt out of their data being held in NCARDRS under Section 251 approval.

More information on the NHR can be found on their website and includes a patient information leaflet.

## Data items and purpose of sharing

Data item	Purpose
Name of newborn screening (NBS) laboratory (from login)	To identify NBS laboratory responsible for testing the sample and making the referral
Contact email address (from login)	As above

Data item	Purpose
Type of centre	To distinguish between nursing and medical centre according to local pathway
Name of centre	To identify correct centre for referral
Contact email address	To notify new referral by email in addition to insystem
Name of nurse/counsellor/doctor	To identify healthcare professional(s) who will receive the referral and for audit purposes
Unique laboratory reference/card serial number	To provide linkage back to the NBS card
NHS number	To identify the baby across NHS care settings
Baby/child’s family name / surname at birth	(Surname at birth) to identify the baby

Baby/child's registered surname (if different)	Surname may change between birth and 42 days (the legal requirement to register the birth)
Baby/child's first name	(First name) to identify the baby
Sex	To identify the baby and to analyse data for difference by gender
Date of birth	To identify the baby and measure performance against KPIs
Gestation of baby at birth	Necessary to interpret baby's screening results
Baby's address line 1	To identify and track baby
Baby's address line 2	As above
Baby's address line 3	As above
Baby's postcode	As above
Ethnic origin	To monitor the disease prevalence by ethnicity and for equality monitoring
Has the baby or child had a blood transfusion?	Necessary to interpret baby's screening results
GP name	To identify and track baby
GP practice code	To identify and track baby
Date of newborn screening test result	To identify the baby and measure performance against KPIs

<b>Data item</b>	<b>Purpose</b>
Newborn screening result	Communicate which condition is suspected
Any other comments on the result	Additional information to clarify result
Mother's NHS number	To improve identification of babies, needed for dataset linkage and quality assurance of linked programme
Mother's surname	As above

Mother's forename	As above
Mother's Hb carrier/affected state	Required to confirm baby's diagnosis in some cases and to evaluate antenatal and newborn linked programme and quality assurance
Father's Hb carrier/affected state	Required to confirm baby's diagnosis in some cases and to evaluate antenatal and newborn linked programme and quality assurance
Prenatal diagnosis (PND) offered/accepted/declined	Evaluate antenatal and newborn linked programme and quality assurance
PND result	Evaluate antenatal and newborn linked programme and quality assurance
Baby/child's hospital number	Unique identifier within an organisation setting
Date NBS results received	To identify the baby and measure performance against KPIs
Date screening result reported to parents	To measure performance against KPIs
Date baby/child attended the haemoglobinopathy medical centre	Confirmation of handover to treatment services and to measure performance against KPIs
Confirmed screening results	Evaluate antenatal and newborn linked programme and quality assurance
Confirmed diagnosis	Evaluate antenatal and newborn linked programme and quality assurance
<b>Data item</b>	<b>Purpose</b>
Date penicillin offered / prescribed/declined (SCD only)	Evaluate antenatal and newborn linked programme and quality assurance
Clinical comments	Additional information to clarify result
Date of death	Evaluate antenatal and newborn linked programme and quality assurance

Cause of death	Evaluate antenatal and newborn linked programme and quality assurance To determine if death can be ascribed to sickle cell disease or thalassaemia
----------------	--

### **Data retention:**

Based on current legal requirements, professional best practice and user needs, data will be retained until the 25<sup>th</sup> birthday<sup>1</sup>.

<https://digital.nhs.uk/data-and-information/looking-after-information/data-security-andinformationgovernance/codes-of-practice-for-handling-information-in-health-andcare/records-management-code-ofpractice-for-health-and-social-care-2016>

## Part B: Terms and conditions

### 1. Call-Off Contract Start date and length

- 1.1 The Supplier must start providing the Services on the date specified in the Order Form.
- 1.2 This Call-Off Contract will expire on the Expiry Date in the Order Form. It will be for up to 24 months from the Start date unless Ended earlier under clause 18 or extended by the Buyer under clause 1.3.
- 1.3 The Buyer can extend this Call-Off Contract, with written notice to the Supplier, by the period in the Order Form, provided that this is within the maximum permitted under the Framework Agreement of 2 periods of up to 12 months each.
- 1.4 The Parties must comply with the requirements under clauses 21.3 to 21.8 if the Buyer reserves the right in the Order Form to extend the contract beyond 24 months.

### 2. Incorporation of terms

- 2.1 The following Framework Agreement clauses (including clauses and defined terms referenced by them) as modified under clause 2.2 are incorporated as separate Call-Off Contract obligations and apply between the Supplier and the Buyer:
  - 4.1 (Warranties and representations)
  - 4.2 to 4.7 (Liability)
  - 4.11 to 4.12 (IR35)
  - 5.4 to 5.5 (Force majeure)
  - 5.8 (Continuing rights)
  - 5.9 to 5.11 (Change of control)
  - 5.12 (Fraud)
  - 5.13 (Notice of fraud)
  - 7.1 to 7.2 (Transparency)
  - 8.3 (Order of precedence)
  - 8.6 (Relationship)
  - 8.9 to 8.11 (Entire agreement)
  - 8.12 (Law and jurisdiction)
  - 8.13 to 8.14 (Legislative change)
  - 8.15 to 8.19 (Bribery and corruption)
  - 8.20 to 8.29 (Freedom of Information Act)
  - 8.30 to 8.31 (Promoting tax compliance)
  - 8.32 to 8.33 (Official Secrets Act)
  - 8.34 to 8.37 (Transfer and subcontracting)
  - 8.40 to 8.43 (Complaints handling and resolution)
  - 8.44 to 8.50 (Conflicts of interest and ethical walls)
  - 8.51 to 8.53 (Publicity and branding)
  - 8.54 to 8.56 (Equality and diversity)
  - 8.59 to 8.60 (Data protection)
  - 8.64 to 8.65 (Severability)

- 8.66 to 8.69 (Managing disputes and Mediation)
- 8.80 to 8.88 (Confidentiality)
- 8.89 to 8.90 (Waiver and cumulative remedies)
- 8.91 to 8.101 (Corporate Social Responsibility)
- paragraphs 1 to 10 of the Framework Agreement glossary and interpretation
- any audit provisions from the Framework Agreement set out by the Buyer in the Order Form

2.2 The Framework Agreement provisions in clause 2.1 will be modified as follows:

2.2.1 a reference to the 'Framework Agreement' will be a reference to the 'Call-Off Contract'

2.2.2 a reference to 'CCS' will be a reference to 'the Buyer'

2.2.3 a reference to the 'Parties' and a 'Party' will be a reference to the Buyer and Supplier as Parties under this Call-Off Contract

2.3 The Parties acknowledge that they are required to complete the applicable Annexes contained in Schedule 4 (Processing Data) of the Framework Agreement for the purposes of this Call-Off Contract. The applicable Annexes being reproduced at Schedule 7 of this Call-Off Contract.

2.4 The Framework Agreement incorporated clauses will be referred to as incorporated Framework clause 'XX', where 'XX' is the Framework Agreement clause number.

2.5 When an Order Form is signed, the terms and conditions agreed in it will be incorporated into this Call-Off Contract.

### 3. Supply of services

3.1 The Supplier agrees to supply the G-Cloud Services and any Additional Services under the terms of the Call-Off Contract and the Supplier's Application.

3.2 The Supplier undertakes that each G-Cloud Service will meet the Buyer's acceptance criteria, as defined in the Order Form.

### 4. Supplier staff

4.1 The Supplier Staff must:

4.1.1 be appropriately experienced, qualified and trained to supply the Services

4.1.2 apply all due skill, care and diligence in faithfully performing those duties

4.1.3 obey all lawful instructions and reasonable directions of the Buyer and provide the Services to the reasonable satisfaction of the Buyer

4.1.4 respond to any enquiries about the Services as soon as reasonably possible

4.1.5 complete any necessary Supplier Staff vetting as specified by the Buyer

4.2 The Supplier must retain overall control of the Supplier Staff so that they are not considered to be employees, workers, agents or contractors of the Buyer.

- 4.3 The Supplier may substitute any Supplier Staff as long as they have the equivalent experience and qualifications to the substituted staff member.
- 4.4 The Buyer may conduct IR35 Assessments using the ESI tool to assess whether the Supplier's engagement under the Call-Off Contract is Inside or Outside IR35.
- 4.5 The Buyer may End this Call-Off Contract for Material Breach as per clause 18.5 hereunder if the Supplier is delivering the Services Inside IR35.
- 4.6 The Buyer may need the Supplier to complete an Indicative Test using the ESI tool before the Start date or at any time during the provision of Services to provide a preliminary view of whether the Services are being delivered Inside or Outside IR35. If the Supplier has completed the Indicative Test, it must download and provide a copy of the PDF with the 14-digit ESI reference number from the summary outcome screen and promptly provide a copy to the Buyer.
- 4.7 If the Indicative Test indicates the delivery of the Services could potentially be Inside IR35, the Supplier must provide the Buyer with all relevant information needed to enable the Buyer to conduct its own IR35 Assessment.
- 4.8 If it is determined by the Buyer that the Supplier is Outside IR35, the Buyer will provide the ESI reference number and a copy of the PDF to the Supplier.

## 5. Due diligence

- 5.1 Both Parties agree that when entering into a Call-Off Contract they:
- 5.1.1 have made their own enquiries and are satisfied by the accuracy of any information supplied by the other Party
  - 5.1.2 are confident that they can fulfil their obligations according to the Call-Off Contract terms
  - 5.1.3 have raised all due diligence questions before signing the Call-Off Contract
  - 5.1.4 have entered into the Call-Off Contract relying on its own due diligence

## 6. Business continuity and disaster recovery

- 6.1 The Supplier will have a clear business continuity and disaster recovery plan in their service descriptions.
- 6.2 The Supplier's business continuity and disaster recovery services are part of the Services and will be performed by the Supplier when required.
- 6.3 If requested by the Buyer prior to entering into this Call-Off Contract, the Supplier must ensure that its business continuity and disaster recovery plan is consistent with the Buyer's own plans.

## 7. Payment, VAT and Call-Off Contract charges

- 7.1 The Buyer must pay the Charges following clauses 7.2 to 7.11 for the Supplier's delivery of the Services.
- 7.2 The Buyer will pay the Supplier within the number of days specified in the Order Form on receipt of a valid invoice.
- 7.3 The Call-Off Contract Charges include all Charges for payment Processing. All invoices submitted to the Buyer for the Services will be exclusive of any Management Charge.



- 7.4 If specified in the Order Form, the Supplier will accept payment for G-Cloud Services by the Government Procurement Card (GPC). The Supplier will be liable to pay any merchant fee levied for using the GPC and must not recover this charge from the Buyer.
- 7.5 The Supplier must ensure that each invoice contains a detailed breakdown of the G-Cloud Services supplied. The Buyer may request the Supplier provides further documentation to substantiate the invoice.
- 7.6 If the Supplier enters into a Subcontract it must ensure that a provision is included in each Subcontract which specifies that payment must be made to the Subcontractor within 30 days of receipt of a valid invoice.
- 7.7 All Charges payable by the Buyer to the Supplier will include VAT at the appropriate Rate.
- 7.8 The Supplier must add VAT to the Charges at the appropriate rate with visibility of the amount as a separate line item.
- 7.9 The Supplier will indemnify the Buyer on demand against any liability arising from the Supplier's failure to account for or to pay any VAT on payments made to the Supplier under this Call-Off Contract. The Supplier must pay all sums to the Buyer at least 5 Working Days before the date on which the tax or other liability is payable by the Buyer.
- 7.10 The Supplier must not suspend the supply of the G-Cloud Services unless the Supplier is entitled to End this Call-Off Contract under clause 18.6 for Buyer's failure to pay undisputed sums of money. Interest will be payable by the Buyer on the late payment of any undisputed sums of money properly invoiced under the Late Payment of Commercial Debts (Interest) Act 1998.
- 7.11 If there's an invoice dispute, the Buyer must pay the undisputed portion of the amount and return the invoice within 10 Working Days of the invoice date. The Buyer will provide a covering statement with proposed amendments and the reason for any non-payment. The Supplier must notify the Buyer within 10 Working Days of receipt of the returned invoice if it accepts the amendments. If it does then the Supplier must provide a replacement valid invoice with the response.
- 7.12 Due to the nature of G-Cloud Services it isn't possible in a static Order Form to exactly define the consumption of services over the duration of the Call-Off Contract. The Supplier agrees that the Buyer's volumes indicated in the Order Form are indicative only.

## 8. Recovery of sums due and right of set-off

- 8.1 If a Supplier owes money to the Buyer, the Buyer may deduct that sum from the Call-Off Contract Charges.

## 9. Insurance

- 9.1 The Supplier will maintain the insurances required by the Buyer including those in this clause.

- 9.2 The Supplier will ensure that:

- 9.2.1 during this Call-Off Contract, Subcontractors hold third party public and products liability insurance of the same amounts that the Supplier would be legally liable to pay as damages, including the claimant's costs and expenses, for accidental death or bodily injury and loss of or damage to Property, to a minimum of £1,000,000

- 9.2.2 the third-party public and products liability insurance contains an 'indemnity to principals' clause for the Buyer's benefit

9.2.3 all agents and professional consultants involved in the Services hold professional indemnity insurance to a minimum indemnity of £1,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

9.2.4 all agents and professional consultants involved in the Services hold employers liability insurance (except where exempt under Law) to a minimum indemnity of £5,000,000 for each individual claim during the Call-Off Contract, and for 6 years after the End or Expiry Date

9.3 If requested by the Buyer, the Supplier will obtain additional insurance policies, or extend existing policies bought under the Framework Agreement.

9.4 If requested by the Buyer, the Supplier will provide the following to show compliance with this clause:

9.4.1 a broker's verification of insurance

9.4.2 receipts for the insurance premium

9.4.3 evidence of payment of the latest premiums due

9.5 Insurance will not relieve the Supplier of any liabilities under the Framework Agreement or this Call-Off Contract and the Supplier will:

9.5.1 take all risk control measures using Good Industry Practice, including the investigation and reports of claims to insurers

9.5.2 promptly notify the insurers in writing of any relevant material fact under any Insurances

9.5.3 hold all insurance policies and require any broker arranging the insurance to hold any insurance slips and other evidence of insurance

9.6 The Supplier will not do or omit to do anything, which would destroy or impair the legal validity of the insurance.

9.7 The Supplier will notify CCS and the Buyer as soon as possible if any insurance policies have been, or are due to be, cancelled, suspended, Ended or not renewed.

9.8 The Supplier will be liable for the payment of any:

9.8.1 premiums, which it will pay promptly

9.8.2 excess or deductibles and will not be entitled to recover this from the Buyer

## 10. Confidentiality

10.1 Subject to clause 24.1 the Supplier must during and after the Term keep the Buyer fully indemnified against all Losses, damages, costs or expenses and other liabilities (including legal fees) arising from any breach of the Supplier's obligations under the Data Protection Legislation or under incorporated Framework Agreement clauses 8.80 to 8.88. The indemnity doesn't apply to the extent that the Supplier breach is due to a Buyer's instruction.

## 11. Intellectual Property Rights

- 11.1 Unless otherwise specified in this Call-Off Contract, a Party will not acquire any right, title or interest in or to the Intellectual Property Rights (IPRs) of the other Party or its Licensors.
- 11.2 The Supplier grants the Buyer a non-exclusive, transferable, perpetual, irrevocable, royalty-free licence to use the Project Specific IPRs and any Background IPRs embedded within the Project Specific IPRs for the Buyer's ordinary business activities.
- 11.3 The Supplier must obtain the grant of any third-party IPRs and Background IPRs so the Buyer can enjoy full use of the Project Specific IPRs, including the Buyer's right to publish the IPR as open source.
- 11.4 The Supplier must promptly inform the Buyer if it can't comply with the clause above and the Supplier must not use third-party IPRs or Background IPRs in relation to the Project Specific IPRs if it can't obtain the grant of a licence acceptable to the Buyer.
- 11.5 The Supplier will, on written demand, fully indemnify the Buyer and the Crown for all Losses which it may incur at any time from any claim of infringement or alleged infringement of a third party's IPRs because of the:
  - 11.5.1 rights granted to the Buyer under this Call-Off Contract
  - 11.5.2 Supplier's performance of the Services
  - 11.5.3 use by the Buyer of the Services
- 11.6 If an IPR Claim is made, or is likely to be made, the Supplier will immediately notify the Buyer in writing and must at its own expense after written approval from the Buyer, either:
  - 11.6.1 modify the relevant part of the Services without reducing its functionality or performance
  - 11.6.2 substitute Services of equivalent functionality and performance, to avoid the infringement or the alleged infringement, as long as there is no additional cost or burden to the Buyer
  - 11.6.3 buy a licence to use and supply the Services which are the subject of the alleged infringement, on terms acceptable to the Buyer
- 11.7 Clause 11.5 will not apply if the IPR Claim is from:
  - 11.7.2 the use of data supplied by the Buyer which the Supplier isn't required to verify under this Call-Off Contract
  - 11.7.3 other material provided by the Buyer necessary for the Services
- 11.8 If the Supplier does not comply with clauses 11.2 to 11.6, the Buyer may End this Call-Off Contract for Material Breach. The Supplier will, on demand, refund the Buyer all the money paid for the affected Services.

## 12. Protection of information

12.1 The Supplier must:

12.1.1 comply with the Buyer's written instructions and this Call-Off Contract when Processing Buyer Personal Data

12.1.2 only Process the Buyer Personal Data as necessary for the provision of the G-Cloud Services or as required by Law or any Regulatory Body

12.1.3 take reasonable steps to ensure that any Supplier Staff who have access to Buyer Personal Data act in compliance with Supplier's security processes

12.2 The Supplier must fully assist with any complaint or request for Buyer Personal Data including by:

12.2.1 providing the Buyer with full details of the complaint or request

12.2.2 complying with a data access request within the timescales in the Data Protection Legislation and following the Buyer's instructions

12.2.3 providing the Buyer with any Buyer Personal Data it holds about a Data Subject (within the timescales required by the Buyer)

12.2.4 providing the Buyer with any information requested by the Data Subject

12.3 The Supplier must get prior written consent from the Buyer to transfer Buyer Personal Data to any other person (including any Subcontractors) for the provision of the G-Cloud Services.

## 13. Buyer data

The Supplier must not remove any proprietary notices in the Buyer Data.

13.1 The Supplier will not store or use Buyer Data except if necessary, to fulfil its obligations.

13.2 If Buyer Data is processed by the Supplier, the Supplier will supply the data to the Buyer as requested.

13.3 The Supplier must ensure that any Supplier system that holds any Buyer Data is a secure system that complies with the Supplier's and Buyer's security policies and all Buyer requirements in the Order Form.

13.4 The Supplier will preserve the integrity of Buyer Data processed by the Supplier and prevent its corruption and loss.

13.4 The Supplier will ensure that any Supplier system which holds any protectively marked Buyer Data or other government data will comply with:

- the principles in the Security Policy Framework at <https://www.gov.uk/government/publications/security-policy-framework> and the Government Security Classification policy at <https://www.gov.uk/government/publications/government-security-classifications>

- guidance issued by the Centre for Protection of National Infrastructure on Risk Management at <https://www.cpni.gov.uk/content/adopt-risk-management-approach> and Protection of Sensitive Information and Assets at <https://www.cpni.gov.uk/protection-sensitive-information-and-assets>
- the National Cyber Security Centre's (NCSC) information risk management guidance, available at <https://www.ncsc.gov.uk/collection/risk-management-collection>
- government best practice in the design and implementation of system components, including network principles, security design principles for digital services and the secure email blueprint, available at <https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice>
- the security requirements of cloud services using the NCSC Cloud Security Principles and

accompanying guidance at <https://www.ncsc.gov.uk/guidance/implementing-cloud-security-principles>

- 13.6 The Buyer will specify any security requirements for this project in the Order Form.
- 13.7 If the Supplier suspects that the Buyer Data has or may become corrupted, lost, breached or significantly degraded in any way for any reason, then the Supplier will notify the Buyer immediately and will (at its own cost if corruption, loss, breach or degradation of the Buyer Data was caused by the action or omission of the Supplier) comply with any remedial action reasonably proposed by the Buyer.
- 13.8 The Supplier agrees to use the appropriate organisational, operational and technological processes to keep the Buyer Data safe from unauthorised use or access, loss, destruction, theft or disclosure.
- 13.9 The provisions of this clause 13 will apply during the term of this Call-Off Contract and for as long as the Supplier holds the Buyer's Data.

## 14. Standards and quality

- 14.1 The Supplier will comply with any standards in this Call-Off Contract, the Order Form and the Framework Agreement.
- 14.2 The Supplier will deliver the Services in a way that enables the Buyer to comply with its obligations under the Technology Code of Practice, which is at:  
<https://www.gov.uk/government/publications/technology-code-of-practice/technology-code-of-practice>
- 14.3 If requested by the Buyer, the Supplier must, at its own cost, ensure that the G-Cloud Services comply with the requirements in the PSN Code of Practice.
- 14.4 If any PSN Services are Subcontracted by the Supplier, the Supplier must ensure that the services have the relevant PSN compliance certification.
- 14.5 The Supplier must immediately disconnect its G-Cloud Services from the PSN if the PSN Authority considers there is a risk to the PSN's security and the Supplier agrees that the Buyer and the PSN Authority will not be liable for any actions, damages, costs, and any other Supplier liabilities which may arise.

## 15. Open source

- 15.1 All software created for the Buyer must be suitable for publication as open source, unless otherwise agreed by the Buyer.
- 15.2 If software needs to be converted before publication as open source, the Supplier must also provide the converted format unless otherwise agreed by the Buyer.

## 16. Security

- 16.1 If requested to do so by the Buyer, before entering into this Call-Off Contract the Supplier will, within 15 Working Days of the date of this Call-Off Contract, develop (and obtain the Buyer's written approval of) a Security Management Plan and an Information Security Management System. After Buyer approval the Security Management Plan and Information Security Management System will apply during the Term of this Call-Off Contract. Both plans will comply with the Buyer's security policy and protect all aspects and processes associated with the delivery of the Services.
- 16.2 The Supplier will use all reasonable endeavours, software and the most up-to-date antivirus definitions available from an industry-accepted antivirus software seller to minimise the impact of Malicious Software.
- 16.3 If Malicious Software causes loss of operational efficiency or loss or corruption of Service Data, the Supplier will help the Buyer to mitigate any losses and restore the Services to operating efficiency as soon as possible.
- 16.4 Responsibility for costs will be at the:
- 16.4.1 Supplier's expense if the Malicious Software originates from the Supplier software or the Service Data while the Service Data was under the control of the Supplier, unless the Supplier can demonstrate that it was already present, not quarantined or identified by the Buyer when provided
- 16.4.2 Buyer's expense if the Malicious Software originates from the Buyer software or the Service Data, while the Service Data was under the Buyer's control
- 16.5 The Supplier will immediately notify the Buyer of any breach of security of Buyer's Confidential Information (and the Buyer of any Buyer Confidential Information breach). Where the breach occurred because of a Supplier Default, the Supplier will recover the Buyer's Confidential Information however it may be recorded.
- 16.6 Any system development by the Supplier should also comply with the government's '10 Steps to Cyber Security' guidance:  
<https://www.ncsc.gov.uk/guidance/10-steps-cyber-security>
- 16.7 If a Buyer has requested in the Order Form that the Supplier has a Cyber Essentials certificate, the Supplier must provide the Buyer with a valid Cyber Essentials certificate (or equivalent) required for the Services before the Start date.

## 17. Guarantee

- 17.1 If this Call-Off Contract is conditional on receipt of a Guarantee that is acceptable to the Buyer, the Supplier must give the Buyer on or before the Start date:
- 17.1.1 an executed Guarantee in the form at Schedule 5
- 17.1.2 a certified copy of the passed resolution or board minutes of the guarantor approving the execution of the Guarantee

## 18. Ending the Call-Off Contract

18.1 The Buyer can End this Call-Off Contract at any time by giving 30 days' written notice to the Supplier, unless a shorter period is specified in the Order Form. The Supplier's obligation to provide the Services will end on the date in the notice.

18.2 The Parties agree that the:

18.2.1 Buyer's right to End the Call-Off Contract under clause 18.1 is reasonable considering the type of cloud Service being provided

18.2.2 Call-Off Contract Charges paid during the notice period is reasonable compensation and covers all the Supplier's avoidable costs or Losses

18.3 Subject to clause 24 (Liability), if the Buyer Ends this Call-Off Contract under clause 18.1, it will indemnify the Supplier against any commitments, liabilities or expenditure which result in any unavoidable Loss by the Supplier, provided that the Supplier takes all reasonable steps to mitigate the Loss. If the Supplier has insurance, the Supplier will reduce its unavoidable costs by any insurance sums available. The Supplier will submit a fully itemised and costed list of the unavoidable Loss with supporting evidence.

18.4 The Buyer will have the right to End this Call-Off Contract at any time with immediate effect by written notice to the Supplier if either the Supplier commits:

18.4.1 a Supplier Default and if the Supplier Default cannot, in the reasonable opinion of the Buyer, be remedied

18.4.2 any fraud

18.5 A Party can End this Call-Off Contract at any time with immediate effect by written notice if:

18.5.1 the other Party commits a Material Breach of any term of this Call-Off Contract (other than failure to pay any amounts due) and, if that breach is remediable, fails to remedy it within 15 Working Days of being notified in writing to do so

18.5.2 an Insolvency Event of the other Party happens

18.5.3 the other Party ceases or threatens to cease to carry on the whole or any material part of its business

18.6 If the Buyer fails to pay the Supplier undisputed sums of money when due, the Supplier must notify the Buyer and allow the Buyer 5 Working Days to pay. If the Buyer doesn't pay within 5 Working Days, the Supplier may End this Call-Off Contract by giving the length of notice in the Order Form.

18.7 A Party who isn't relying on a Force Majeure event will have the right to End this Call-Off Contract if clause 23.1 applies.

## 19. Consequences of suspension, ending and expiry

19.1 If a Buyer has the right to End a Call-Off Contract, it may elect to suspend this Call-Off Contract or any part of it.



- 19.2 Even if a notice has been served to End this Call-Off Contract or any part of it, the Supplier must continue to provide the Ordered G-Cloud Services until the dates set out in the notice.
- 19.3 The rights and obligations of the Parties will cease on the Expiry Date or End Date whichever applies) of this Call-Off Contract, except those continuing provisions described in clause 19.4.
- 19.4 Ending or expiry of this Call-Off Contract will not affect:
- 19.4.1 any rights, remedies or obligations accrued before its Ending or expiration
- 19.4.2 the right of either Party to recover any amount outstanding at the time of Ending or expiry
- 19.4.3 the continuing rights, remedies or obligations of the Buyer or the Supplier under clauses
- 7 (Payment, VAT and Call-Off Contract charges)
  - 8 (Recovery of sums due and right of set-off)
  - 9 (Insurance)
  - 10 (Confidentiality)
  - 11 (Intellectual property rights)
  - 12 (Protection of information)
  - 13 (Buyer data)
  - 19 (Consequences of suspension, ending and expiry)
  - 24 (Liability); incorporated Framework Agreement clauses: 4.2 to 4.7 (Liability)
  - 8.44 to 8.50 (Conflicts of interest and ethical walls)
  - 8.89 to 8.90 (Waiver and cumulative remedies)
- 19.4.4 any other provision of the Framework Agreement or this Call-Off Contract which expressly or by implication is in force even if it Ends or expires
- 19.5 At the end of the Call-Off Contract Term, the Supplier must promptly:
- 19.5.1 return all Buyer Data including all copies of Buyer software, code and any other software licensed by the Buyer to the Supplier under it
- 19.5.2 return any materials created by the Supplier under this Call-Off Contract if the IPRs are owned by the Buyer
- 19.5.3 stop using the Buyer Data and, at the direction of the Buyer, provide the Buyer with a complete and uncorrupted version in electronic form in the formats and on media agreed with the Buyer
- 19.5.4 destroy all copies of the Buyer Data when they receive the Buyer's written instructions to do so or 12 calendar months after the End or Expiry Date, and provide written confirmation to the Buyer that the data has been securely destroyed, except if the retention of Buyer Data is required by Law
- 19.5.5 work with the Buyer on any ongoing work
- 19.5.6 return any sums prepaid for Services which have not been delivered to the Buyer, within 10 Working Days of the End or Expiry Date

- 19.6 Each Party will return all of the other Party's Confidential Information and confirm this has been done, unless there is a legal requirement to keep it or this Call-Off Contract states otherwise.
- 19.7 All licences, leases and authorisations granted by the Buyer to the Supplier will cease at the end of the Call-Off Contract Term without the need for the Buyer to serve notice except if this Call-Off Contract states otherwise.

## 20. Notices

- 20.1 Any notices sent must be in writing. For the purpose of this clause, an email is accepted as being 'in writing'.

Manner of delivery	Deemed time of delivery	Proof of service
Email	9am on the first Working Day after sending	Sent by pdf to the correct email address without getting an error message

- 20.2 This clause does not apply to any legal action or other method of dispute resolution which should be sent to the addresses in the Order Form (other than a dispute notice under this Call-Off Contract).

## 21. Exit plan

- 21.1 The Supplier must provide an exit plan in its Application which ensures continuity of service and the Supplier will follow it.
- 21.2 When requested, the Supplier will help the Buyer to migrate the Services to a replacement supplier in line with the exit plan. This will be at the Supplier's own expense if the Call-Off Contract Ended before the Expiry Date due to Supplier cause.
- 21.3 If the Buyer has reserved the right in the Order Form to extend the Call-Off Contract Term beyond 24 months the Supplier must provide the Buyer with an additional exit plan for approval by the Buyer at least 8 weeks before the 18 month anniversary of the Start date.
- 21.4 The Supplier must ensure that the additional exit plan clearly sets out the Supplier's methodology for achieving an orderly transition of the Services from the Supplier to the Buyer or its replacement Supplier at the expiry of the proposed extension period or if the contract Ends during that period.
- 21.5 Before submitting the additional exit plan to the Buyer for approval, the Supplier will work with the Buyer to ensure that the additional exit plan is aligned with the Buyer's own exit plan and strategy.
- 21.6 The Supplier acknowledges that the Buyer's right to extend the Term beyond 24 months is subject to the Buyer's own governance process. Where the Buyer is a central government department, this includes the need to obtain approval from GDS under the Spend Controls

process. The approval to extend will only be given if the Buyer can clearly demonstrate that the Supplier's additional exit plan ensures that:

21.6.1 the Buyer will be able to transfer the Services to a replacement supplier before the expiry or Ending of the extension period on terms that are commercially reasonable and acceptable to the Buyer

21.6.2 there will be no adverse impact on service continuity

21.6.3 there is no vendor lock-in to the Supplier's Service at exit

21.6.4 it enables the Buyer to meet its obligations under the Technology Code Of Practice

21.7 If approval is obtained by the Buyer to extend the Term, then the Supplier will comply with its obligations in the additional exit plan.

21.8 The additional exit plan must set out full details of timescales, activities and roles and responsibilities of the Parties for:

21.8.1 the transfer to the Buyer of any technical information, instructions, manuals and code reasonably required by the Buyer to enable a smooth migration from the Supplier

21.8.2 the strategy for exportation and migration of Buyer Data from the Supplier system to the Buyer or a replacement supplier, including conversion to open standards or other standards required by the Buyer

21.8.3 the transfer of Project Specific IPR items and other Buyer customisations, configurations and databases to the Buyer or a replacement supplier

21.8.4 the testing and assurance strategy for exported Buyer Data

21.8.5 if relevant, TUPE-related activity to comply with the TUPE regulations

21.8.6 any other activities and information which is reasonably required to ensure continuity of Service during the exit period and an orderly transition

## **22. Handover to replacement supplier**

22.1 At least 10 Working Days before the Expiry Date or End Date, the Supplier must provide any:

22.1.1 data (including Buyer Data), Buyer Personal Data and Buyer Confidential Information in the Supplier's possession, power or control

22.1.2 other information reasonably requested by the Buyer

22.2 On reasonable notice at any point during the Term, the Supplier will provide any information and data about the G-Cloud Services reasonably requested by the Buyer (including information on volumes, usage, technical aspects, service performance and staffing). This will help the Buyer understand how the Services have been provided and to run a fair competition for a new supplier.

- 22.3 This information must be accurate and complete in all material respects and the level of detail must be sufficient to reasonably enable a third party to prepare an informed offer for replacement services and not be unfairly disadvantaged compared to the Supplier in the buying process.

## 23. Force majeure

- 23.1 If a Force Majeure event prevents a Party from performing its obligations under this Call-Off Contract for more than the number of consecutive days set out in the Order Form, the other Party may End this Call-Off Contract with immediate effect by written notice.

## 24. Liability

- 24.1 Subject to incorporated Framework Agreement clauses 4.2 to 4.7, each Party's Yearly total liability for Defaults under or in connection with this Call-Off Contract (whether expressed as an indemnity or otherwise) will be set as follows:

24.1.1 Property: for all Defaults by either party resulting in direct loss to the property (including technical infrastructure, assets, IPR or equipment but excluding any loss or damage to Buyer Data) of the other Party, will not exceed the amount in the Order Form

24.1.2 Buyer Data: for all Defaults by the Supplier resulting in direct loss, destruction, corruption, degradation or damage to any Buyer Data, will not exceed the amount in the Order Form

24.1.3 Other Defaults: for all other Defaults by either party, claims, Losses or damages, whether arising from breach of contract, misrepresentation (whether under common law or statute), tort (including negligence), breach of statutory duty or otherwise will not exceed the amount in the Order Form.

## 25. Premises

- 25.1 If either Party uses the other Party's premises, that Party is liable for all loss or damage it causes to the premises. It is responsible for repairing any damage to the premises or any objects on the premises, other than fair wear and tear.

- 25.2 The Supplier will use the Buyer's premises solely for the performance of its obligations under this Call-Off Contract.

- 25.3 The Supplier will vacate the Buyer's premises when the Call-Off Contract Ends or expires.

25.4 This clause does not create a tenancy or exclusive right of occupation.

25.5 While on the Buyer's premises, the Supplier will:

25.5.1 comply with any security requirements at the premises and not do anything to weaken the security of the premises

25.5.2 comply with Buyer requirements for the conduct of personnel

25.5.3 comply with any health and safety measures implemented by the Buyer

25.5.4 immediately notify the Buyer of any incident on the premises that causes any damage to Property which could cause personal injury

25.6 The Supplier will ensure that its health and safety policy statement (as required by the Health and Safety at Work etc Act 1974) is made available to the Buyer on request.

## 26. Equipment

26.1 The Supplier is responsible for providing any Equipment which the Supplier requires to provide the Services.

26.2 Any Equipment brought onto the premises will be at the Supplier's own risk and the Buyer will have no liability for any loss of, or damage to, any Equipment.

26.3 When the Call-Off Contract Ends or expires, the Supplier will remove the Equipment and any other materials leaving the premises in a safe and clean condition.

## 27. The Contracts (Rights of Third Parties) Act 1999

27.1 Except as specified in clause 29.8, a person who isn't Party to this Call-Off Contract has no right under the Contracts (Rights of Third Parties) Act 1999 to enforce any of its terms. This does not affect any right or remedy of any person which exists or is available otherwise.

## 28. Environmental requirements

28.1 The Buyer will provide a copy of its environmental policy to the Supplier on request, which the Supplier will comply with.

28.2 The Supplier must provide reasonable support to enable Buyers to work in an environmentally friendly way, for example by helping them recycle or lower their carbon footprint.

## 29. The Employment Regulations (TUPE)

29.1 The Supplier agrees that if the Employment Regulations apply to this Call-Off Contract on the Start date then it must comply with its obligations under the Employment Regulations and (if applicable) New Fair Deal (including entering into an Admission Agreement) and will indemnify the Buyer or any Former Supplier for any loss arising from any failure to comply.

29.2 Twelve months before this Call-Off Contract expires, or after the Buyer has given notice to End it, and within 28 days of the Buyer's request, the Supplier will fully and accurately disclose to the Buyer all staff information including, but not limited to, the total number of staff assigned for the purposes of TUPE to the Services. For each person identified the Supplier must provide details of:

- 29.2.1 the activities they perform
- 29.2.2 age
- 29.2.3 start date
- 29.2.4 place of work

- 29.2.5 notice period
- 29.2.6 redundancy payment entitlement
- 29.2.7 salary, benefits and pension entitlements
- 29.2.8 employment status
- 29.2.9 identity of employer
- 29.2.10 working arrangements
- 29.2.11 outstanding liabilities
- 29.2.12 sickness absence
- 29.2.13 copies of all relevant employment contracts and related documents
- 29.2.14 all information required under regulation 11 of TUPE or as reasonably requested by the Buyer

- 29.3 The Supplier warrants the accuracy of the information provided under this TUPE clause and will notify the Buyer of any changes to the amended information as soon as reasonably possible. The Supplier will permit the Buyer to use and disclose the information to any prospective Replacement Supplier.
- 29.4 In the 12 months before the expiry of this Call-Off Contract, the Supplier will not change the identity and number of staff assigned to the Services (unless reasonably requested by the Buyer) or their terms and conditions, other than in the ordinary course of business.
- 29.5 The Supplier will co-operate with the re-tendering of this Call-Off Contract by allowing the Replacement Supplier to communicate with and meet the affected employees or their representatives.
- 29.6 The Supplier will indemnify the Buyer or any Replacement Supplier for all Loss arising from both:
  - 29.6.1 its failure to comply with the provisions of this clause
  - 29.6.2 any claim by any employee or person claiming to be an employee (or their employee representative) of the Supplier which arises or is alleged to arise from any act or omission by the Supplier on or before the date of the Relevant Transfer
- 29.7 The provisions of this clause apply during the Term of this Call-Off Contract and indefinitely after it Ends or expires.
- 29.8 For these TUPE clauses, the relevant third party will be able to enforce its rights under this clause but their consent will not be required to vary these clauses as the Buyer and Supplier may agree.

## 30. Additional G-Cloud services

- 30.1 The Buyer may require the Supplier to provide Additional Services. The Buyer doesn't have to buy any Additional Services from the Supplier and can buy services that are the same as or similar to the Additional Services from any third party.
- 30.2 If reasonably requested to do so by the Buyer in the Order Form, the Supplier must provide and monitor performance of the Additional Services using an Implementation Plan.

## 31. Collaboration

- 31.1 If the Buyer has specified in the Order Form that it requires the Supplier to enter into a Collaboration Agreement, the Supplier must give the Buyer an executed Collaboration Agreement before the Start date.
- 31.2 In addition to any obligations under the Collaboration Agreement, the Supplier must:
  - 31.2.1 work proactively and in good faith with each of the Buyer's contractors
  - 31.2.2 co-operate and share information with the Buyer's contractors to enable the efficient operation of the Buyer's ICT services and G-Cloud Services

## 32. Variation process

- 32.1 The Buyer can request in writing a change to this Call-Off Contract if it isn't a material change to the Framework Agreement/or this Call-Off Contract. Once implemented, it is called a Variation.
- 32.2 The Supplier must notify the Buyer immediately in writing of any proposed changes to their G-Cloud Services or their delivery by submitting a Variation request. This includes any changes in the Supplier's supply chain.
- 32.3 If Either Party can't agree to or provide the Variation, the Buyer may agree to continue performing its obligations under this Call-Off Contract without the Variation, or End this Call- Off Contract by giving 30 days notice to the Supplier.

## 33. Data Protection Legislation (GDPR)

- 33.1 Pursuant to clause 2.1 and for the avoidance of doubt, clauses 8.59 and 8.60 of the Framework Agreement are incorporated into this Call-Off Contract. For reference, the appropriate GDPR templates which are required to be completed in accordance with

## Schedule 3: Collaboration agreement

The Collaboration agreement is available at <https://www.gov.uk/guidance/g-cloud-templates-and-legal-documents>

## Schedule 4: Alternative clauses

The Alternative clauses are available at <https://www.gov.uk/guidance/g-cloud-templates-and-legal-documents>

## Schedule 5: Guarantee

The Guarantee is available at <https://www.gov.uk/guidance/g-cloud-templates-and-legal-documents>

## Schedule 6: Glossary and interpretations

In this Call-Off Contract the following expressions mean:

Expression	Meaning
<b>Additional Services</b>	Any services ancillary to the G-Cloud Services that are in the scope of Framework Agreement Section 2 (Services Offered) which a Buyer may request.
<b>Admission Agreement</b>	The agreement to be entered into to enable the Supplier to participate in the relevant Civil Service pension scheme(s).
<b>Application</b>	The response submitted by the Supplier to the Invitation to Tender (known as the Invitation to Apply on the Digital Marketplace).
<b>Audit</b>	An audit carried out under the incorporated Framework Agreement clauses specified by the Buyer in the Order (if any).

<b>Background IPRs</b>	<p>For each Party, IPRs:</p> <ul style="list-style-type: none"> <li>owned by that Party before the date of this Call-Off Contract (as may be enhanced and/or modified but not as a consequence of the Services) including IPRs contained in any of the Party's Know-How, documentation and processes</li> <li>created by the Party independently of this Call-Off Contract, or</li> </ul> <p>For the Buyer, Crown Copyright which isn't available to the Supplier otherwise than under this Call-Off Contract, but excluding IPRs owned by that Party in Buyer software or Supplier software.</p>
<b>Buyer</b>	The contracting authority ordering services as set out in the Order Form.
<b>Buyer Data</b>	All data supplied by the Buyer to the Supplier including Personal Data and Service Data that is owned and managed by the Buyer.
<b>Buyer Personal Data</b>	The Personal Data supplied by the Buyer to the Supplier for purposes of, or in connection with, this Call-Off Contract.
<b>Buyer Representative</b>	The representative appointed by the Buyer under this Call-Off Contract.



<b>Buyer Software</b>	Software owned by or licensed to the Buyer (other than under this Agreement), which is or will be used by the Supplier to provide the Services.
<b>Call-Off Contract</b>	This call-off contract entered into following the provisions of the Framework Agreement for the provision of Services made between the Buyer and the Supplier comprising the Order Form, the Call-Off terms and conditions, the Call-Off schedules and the Collaboration Agreement.
<b>Charges</b>	The prices (excluding any applicable VAT), payable to the Supplier by the Buyer under this Call-Off Contract.
<b>Collaboration Agreement</b>	An agreement, substantially in the form set out at Schedule 3, between the Buyer and any combination of the Supplier and contractors, to ensure collaborative working in their delivery of the Buyer's Services and to ensure that the Buyer receives end-to-end services across its IT estate.
<b>Commercially Sensitive Information</b>	Information, which the Buyer has been notified about by the Supplier in writing before the Start date with full details of why the Information is deemed to be commercially sensitive.

<b>Confidential Information</b>	<p>Data, Personal Data and any information, which may include (but isn't limited to) any:</p> <ul style="list-style-type: none"> <li>information about business, affairs, developments, trade secrets, know-how, personnel, and third parties, including all Intellectual Property Rights (IPRs), together with all information derived from any of the above</li> <li>other information clearly designated as being confidential or which ought reasonably be considered to be confidential (whether or not it is marked 'confidential').</li> </ul>
<b>Control</b>	'Control' as defined in section 1124 and 450 of the Corporation Tax Act 2010. 'Controls' and 'Controlled' will be interpreted accordingly.
<b>Controller</b>	Takes the meaning given in the GDPR.

<b>Crown</b>	The government of the United Kingdom (including the Northern Ireland Assembly and Executive Committee, the Scottish Executive and the National Assembly for Wales), including, but not limited to, government ministers and government departments and particular bodies, persons, commissions or agencies carrying out functions on its behalf.
<b>Data Loss Event</b>	Event that results, or may result, in unauthorised access to Personal Data held by the Processor under this Framework Agreement and/or actual or potential loss and/or destruction of Personal Data in breach of this Agreement, including any Personal Data Breach.
<b>Data Protection Impact Assessment (DPIA)</b>	An assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data.
<b>Data Protection Legislation (DPL)</b>	Data Protection Legislation means: (i) the GDPR, the LED and any applicable national implementing Laws as amended from time to time (ii) the DPA 2018 to the extent that it relates to Processing of Personal Data and privacy (iii) all applicable Law about the Processing of Personal Data and privacy including if applicable legally binding guidance and codes of practice issued by the Information Commissioner
<b>Data Subject</b>	Takes the meaning given in the GDPR

<b>Default</b>	<p>Default is any:</p> <ul style="list-style-type: none"> <li>• breach of the obligations of the Supplier (including any fundamental breach or breach of a fundamental term)</li> <li>• other Default, negligence or negligent statement of the Supplier, of its Subcontractors or any Supplier Staff (whether by act or omission), in connection with or in relation to this Call-Off Contract</li> </ul> <p>Unless otherwise specified in the Framework Agreement the Supplier is liable to CCS for a Default of the Framework Agreement and in relation to a Default of the Call-Off Contract, the Supplier is liable to the Buyer.</p>
<b>Deliverable(s)</b>	The G-Cloud Services the Buyer contracts the Supplier to provide under this Call-Off Contract.

<b>Digital Marketplace</b>	The government marketplace where Services are available for Buyers to buy. ( <a href="https://www.digitalmarketplace.service.gov.uk/">https://www.digitalmarketplace.service.gov.uk/</a> )
<b>DPA 2018</b>	Data Protection Act 2018.
<b>Employment Regulations</b>	The Transfer of Undertakings (Protection of Employment) Regulations 2006 (SI 2006/246) ('TUPE') which implements the Acquired Rights Directive.
<b>End</b>	Means to terminate; and Ended and Ending are construed accordingly.
<b>Environmental Information Regulations or EIR</b>	The Environmental Information Regulations 2004 together with any guidance or codes of practice issued by the Information Commissioner or relevant government department about the regulations.
<b>Equipment</b>	The Supplier's hardware, computer and telecoms devices, plant, materials and such other items supplied and used by the Supplier (but not hired, leased or loaned from CCS or the Buyer) in the performance of its obligations under this Call-Off Contract.
<b>ESI Reference Number</b>	The 14 digit ESI reference number from the summary of the outcome screen of the ESI tool.
<b>Employment Status Indicator test tool or ESI tool</b>	The HMRC Employment Status Indicator test tool. The most up-to-date version must be used. At the time of drafting the tool may be found here: <a href="https://www.gov.uk/guidance/check-employment-status-for-tax">https://www.gov.uk/guidance/check-employment-status-for-tax</a>
<b>Expiry Date</b>	The expiry date of this Call-Off Contract in the Order Form.

<b>Force Majeure</b>	<p>A force Majeure event means anything affecting either Party's performance of their obligations arising from any:</p> <ul style="list-style-type: none"> <li>• acts, events or omissions beyond the reasonable control of the affected Party</li> <li>• riots, war or armed conflict, acts of terrorism, nuclear, biological or chemical warfare</li> <li>• acts of government, local government or Regulatory Bodies</li> <li>• fire, flood or disaster and any failure or shortage of power or fuel</li> <li>• industrial dispute affecting a third party for which a substitute third party isn't reasonably available</li> </ul> <p>The following do not constitute a Force Majeure event:</p> <ul style="list-style-type: none"> <li>• any industrial dispute about the Supplier, its staff, or failure in the Supplier's (or a Subcontractor's) supply chain</li> <li>• any event which is attributable to the wilful act, neglect or failure to take reasonable precautions by the Party seeking to rely on Force Majeure</li> <li>• the event was foreseeable by the Party seeking to rely on Force Majeure at the time this Call-Off Contract was entered into</li> <li>• any event which is attributable to the Party seeking to rely on Force Majeure and its failure to comply with its own business continuity and disaster recovery plans</li> </ul>
<b>Former Supplier</b>	A supplier supplying services to the Buyer before the Start date that are the same as or substantially similar to the Services. This also includes any Subcontractor or the Supplier (or any subcontractor of the Subcontractor).
<b>Framework Agreement</b>	The clauses of framework agreement RM1557.12 together with the Framework Schedules.
<b>Fraud</b>	Any offence under Laws creating offences in respect of fraudulent acts (including the Misrepresentation Act 1967) or at common law in respect of fraudulent acts in relation to this Call-Off Contract or defrauding or attempting to defraud or conspiring to defraud the Crown.
<b>Freedom of Information Act or FoIA</b>	The Freedom of Information Act 2000 and any subordinate legislation made under the Act together with any guidance or codes of practice issued by the Information Commissioner or relevant government department in relation to the legislation.
<b>G-Cloud Services</b>	The cloud services described in Framework Agreement Section 2 (Services Offered) as defined by the Service Definition, the Supplier Terms and any related Application documentation, which the

	Supplier must make available to CCS and Buyers and those services which are deliverable by the Supplier under the Collaboration Agreement.
<b>GDPR</b>	General Data Protection Regulation (Regulation (EU) 2016/679)
<b>Good Industry Practice</b>	Standards, practices, methods and process conforming to the Law and the exercise of that degree of skill and care, diligence, prudence and foresight which would reasonably and ordinarily be expected from a skilled and experienced person or body engaged in a similar undertaking in the same or similar circumstances.
<b>Government Procurement Card</b>	The government's preferred method of purchasing and payment for low value goods or services.
<b>Guarantee</b>	The guarantee described in Schedule 5.
<b>Guidance</b>	Any current UK government guidance on the Public Contracts Regulations 2015. In the event of a conflict between any current UK government guidance and the Crown Commercial Service guidance, current UK government guidance will take precedence.
<b>Implementation Plan</b>	The plan with an outline of processes (including data standards for migration), costs (for example) of implementing the services which may be required as part of Onboarding.
<b>Indicative test</b>	ESI tool completed by contractors on their own behalf at the request of CCS or the Buyer (as applicable) under clause 4.6.
<b>Information</b>	Has the meaning given under section 84 of the Freedom of Information Act 2000.
<b>Information security management system</b>	The information security management system and process developed by the Supplier in accordance with clause 16.1.
<b>Inside IR35</b>	Contractual engagements which would be determined to be within the scope of the IR35 Intermediaries legislation if assessed using the ESI tool.

<b>Insolvency event</b>	<p>Can be:</p> <ul style="list-style-type: none"> <li>• a voluntary arrangement</li> <li>• a winding-up petition</li> <li>• the appointment of a receiver or administrator</li> <li>• an unresolved statutory demand</li> <li>• a Schedule A1 moratorium</li> </ul>
<b>Intellectual Property Rights or IPR</b>	<p>Intellectual Property Rights are:</p> <ul style="list-style-type: none"> <li>• copyright, rights related to or affording protection similar to copyright, rights in databases, patents and rights in inventions, semi-conductor topography rights, trade marks, rights in internet domain names and website addresses and other rights in trade names, designs, Know-How, trade secrets and other rights in Confidential Information</li> <li>• applications for registration, and the right to apply for registration, for any of the rights listed at (a) that are capable of being registered in any country or jurisdiction</li> <li>• all other rights having equivalent or similar effect in any country or jurisdiction</li> </ul>
<b>Intermediary</b>	<p>For the purposes of the IR35 rules an intermediary can be:</p> <ul style="list-style-type: none"> <li>• the supplier's own limited company</li> <li>• a service or a personal service company</li> <li>• a partnership</li> </ul> <p>It does not apply if you work for a client through a Managed Service Company (MSC) or agency (for example, an employment agency).</p>
<b>IPR claim</b>	As set out in clause 11.5.
<b>IR35</b>	IR35 is also known as 'Intermediaries legislation'. It's a set of rules that affect tax and National Insurance where a Supplier is contracted to work for a client through an Intermediary.
<b>IR35 assessment</b>	Assessment of employment status using the ESI tool to determine if engagement is Inside or Outside IR35.
<b>Know-How</b>	All ideas, concepts, schemes, information, knowledge, techniques, methodology, and anything else in the nature of know-how relating to the G-Cloud Services but excluding know-how already in the Supplier's or CCS's possession before the Start date.

<b>Law</b>	Any law, subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the relevant Party is bound to comply.
<b>LED</b>	Law Enforcement Directive (EU) 2016/680.

<b>Loss</b>	All losses, liabilities, damages, costs, expenses (including legal fees), disbursements, costs of investigation, litigation, settlement, judgment, interest and penalties whether arising in contract, tort (including negligence), breach of statutory duty, misrepresentation or otherwise and ' <b>Losses</b> ' will be interpreted accordingly.
<b>Lot</b>	Any of the 3 Lots specified in the ITT and Lots will be construed accordingly.
<b>Malicious Software</b>	Any software program or code intended to destroy, interfere with, corrupt, or cause undesired effects on program files, data or other information, executable code or application software macros, whether or not its operation is immediate or delayed, and whether the malicious software is introduced wilfully, negligently or without knowledge of its existence.
<b>Management Charge</b>	The sum paid by the Supplier to CCS being an amount of up to 1% but currently set at 0.75% of all Charges for the Services invoiced to Buyers (net of VAT) in each month throughout the duration of the Framework Agreement and thereafter, until the expiry or End of any Call-Off Contract.
<b>Management Information</b>	The management information specified in Framework Agreement section 6 (What you report to CCS).
<b>Material Breach</b>	Those breaches which have been expressly set out as a Material Breach and any other single serious breach or persistent failure to perform as required under this Call-Off Contract.
<b>Ministry of Justice Code</b>	The Ministry of Justice's Code of Practice on the Discharge of the Functions of Public Authorities under Part 1 of the Freedom of Information Act 2000.

<b>New Fair Deal</b>	The revised Fair Deal position in the HM Treasury guidance: “Fair Deal for staff pensions: staff transfer from central government” issued in October 2013 as amended.
<b>Order</b>	An order for G-Cloud Services placed by a contracting body with the Supplier in accordance with the ordering processes.
<b>Order Form</b>	The order form set out in Part A of the Call-Off Contract to be used by a Buyer to order G-Cloud Services.
<b>Ordered G-Cloud Services</b>	G-Cloud Services which are the subject of an order by the Buyer.

<b>Outside IR35</b>	Contractual engagements which would be determined to not be within the scope of the IR35 intermediaries legislation if assessed using the ESI tool.
<b>Party</b>	The Buyer or the Supplier and ‘Parties’ will be interpreted accordingly.
<b>Personal Data</b>	Takes the meaning given in the GDPR.
<b>Personal Data Breach</b>	Takes the meaning given in the GDPR.
<b>Processing</b>	Takes the meaning given in the GDPR.
<b>Processor</b>	Takes the meaning given in the GDPR.
<b>Prohibited act</b>	<p>To directly or indirectly offer, promise or give any person working for or engaged by a Buyer or CCS a financial or other advantage to:</p> <ul style="list-style-type: none"> <li>• induce that person to perform improperly a relevant function or activity</li> <li>• reward that person for improper performance of a relevant function or activity</li> <li>• commit any offence: <ul style="list-style-type: none"> <li>○ under the Bribery Act 2010</li> <li>○ under legislation creating offences concerning Fraud</li> <li>○ at common Law concerning Fraud</li> <li>○ committing or attempting or conspiring to commit Fraud</li> </ul> </li> </ul>



<b>Project Specific IPRs</b>	Any intellectual property rights in items created or arising out of the performance by the Supplier (or by a third party on behalf of the Supplier) specifically for the purposes of this Call-Off Contract including databases, configurations, code, instructions, technical documentation and schema but not including the Supplier's Background IPRs.
<b>Property</b>	Assets and property including technical infrastructure, IPRs and equipment.
<b>Protective Measures</b>	Appropriate technical and organisational measures which may include: pseudonymisation and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.

<b>PSN or Public Services Network</b>	The Public Services Network (PSN) is the government's high-performance network which helps public sector organisations work together, reduce duplication and share resources.
<b>Regulatory body or bodies</b>	Government departments and other bodies which, whether under statute, codes of practice or otherwise, are entitled to investigate or influence the matters dealt with in this Call-Off Contract.
<b>Relevant person</b>	Any employee, agent, servant, or representative of the Buyer, any other public body or person employed by or on behalf of the Buyer, or any other public body.
<b>Relevant Transfer</b>	A transfer of employment to which the employment regulations applies.
<b>Replacement Services</b>	Any services which are the same as or substantially similar to any of the Services and which the Buyer receives in substitution for any of the services after the expiry or Ending or partial Ending of the Call-Off Contract, whether those services are provided by the Buyer or a third party.
<b>Replacement supplier</b>	Any third-party service provider of replacement services appointed by the Buyer (or where the Buyer is providing replacement Services for its own account, the Buyer).

<b>Security management plan</b>	The Supplier's security management plan developed by the Supplier in accordance with clause 16.1.
<b>Services</b>	The services ordered by the Buyer as set out in the Order Form.
<b>Service data</b>	Data that is owned or managed by the Buyer and used for the G-Cloud Services, including backup data.
<b>Service definition(s)</b>	The definition of the Supplier's G-Cloud Services provided as part of their Application that includes, but isn't limited to, those items listed in Section 2 (Services Offered) of the Framework Agreement.
<b>Service description</b>	The description of the Supplier service offering as published on the Digital Marketplace.
<b>Service Personal Data</b>	The Personal Data supplied by a Buyer to the Supplier in the course of the use of the G-Cloud Services for purposes of or in connection with this Call-Off Contract.

<b>Spend controls</b>	The approval process used by a central government Buyer if it needs to spend money on certain digital or technology services, see <a href="https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service">https://www.gov.uk/service-manual/agile-delivery/spend-controls-check-if-you-need-approval-to-spend-money-on-a-service</a>
<b>Start date</b>	The Start date of this Call-Off Contract as set out in the Order Form.
<b>Subcontract</b>	Any contract or agreement or proposed agreement between the Supplier and a subcontractor in which the subcontractor agrees to provide to the Supplier the G-Cloud Services or any part thereof or facilities or goods and services necessary for the provision of the G-Cloud Services or any part thereof.
<b>Subcontractor</b>	Any third party engaged by the Supplier under a subcontract (permitted under the Framework Agreement and the Call-Off Contract) and its servants or agents in connection with the provision of G-Cloud Services.
<b>Subprocessor</b>	Any third party appointed to process Personal Data on behalf of the Supplier under this Call-Off Contract.
<b>Supplier</b>	The person, firm or company identified in the Order Form.

<b>Supplier Representative</b>	The representative appointed by the Supplier from time to time in relation to the Call-Off Contract.
<b>Supplier staff</b>	All persons employed by the Supplier together with the Supplier's servants, agents, suppliers and subcontractors used in the performance of its obligations under this Call-Off Contract.
<b>Supplier terms</b>	The relevant G-Cloud Service terms and conditions as set out in the Terms and Conditions document supplied as part of the Supplier's Application.
<b>Term</b>	The term of this Call-Off Contract as set out in the Order Form.
<b>Variation</b>	This has the meaning given to it in clause 32 (Variation process).
<b>Working Days</b>	Any day other than a Saturday, Sunday or public holiday in England and Wales.
<b>Year</b>	A contract year.

## Schedule 7: GDPR Information

### Appendix 4:

#### Data Flows and Data Sharing

The newborn outcomes system automates referral of infants that screen positive for sickle cell disease and thalassaemia and supports the collection and reporting of data. It replaces existing data flows used to support the newborn outcomes project previously run by KCL and currently held by NCARDS, PHE and includes the same data set.

The referral is created in the screening laboratory and shared with clinical centre(s) depending on local pathway. Data is added to the record by clinical teams.

Removing the need for clinicians to enter the same data twice (e.g. demographics, screening results, etc.) is one of the key requirements for the project. To enable integration with the NHR people who already have a user account on the NHR, will access the SCT Newborn Outcomes system through an interface in the NHR rather than logging in to a separate system.

The interface in the NHR matches the main SCT Newborn Outcomes System, and is provided as a 'view' onto the system for NHR users.

#### Data flows:



This interface is provided as a convenience function to allow NHR users to view and use the SCT Newborn Outcomes System without a separate login. It does not affect the process or data collected. All data is held in the Newborn Outcomes System. The NHR is a consented register and no data crosses into the NHR until consent has been explicitly recorded (**point 5**). The Newborn Outcomes system collects only a minimum data set additional data items recorded on the NHR are not shared back.

De-personalised KPI data reports (**point 3**), are returned to the NHS SCT screening programme.

Information about what personally identifiable information is used by the screening programmes and why is provided in “[Screening tests for you and your baby](#)”, a booklet issued to all pregnant women in England with more detailed information on

[Gov.UK](#). This includes the parent’s right to opt out of their data being held in NCARDS under Section 251 approval.

More information on the [NHR](#) can be found on their website and includes [a patient information leaflet](#).

## Data items and purpose of sharing

Data item	Purpose
Name of newborn screening (NBS) laboratory (from login)	To identify NBS laboratory responsible for testing the sample and making the referral
Contact email address (from login)	As above

Data item	Purpose
Type of centre	To distinguish between nursing and medical centre according to local pathway
Name of centre	To identify correct centre for referral
Contact email address	To notify new referral by email in addition to insystem
Name of nurse/counsellor/doctor	To identify healthcare professional(s) who will receive the referral and for audit purposes
Unique laboratory reference/card serial number	To provide linkage back to the NBS card
NHS number	To identify the baby across NHS care settings
Baby/child’s family name / surname at birth	(Surname at birth) to identify the baby

Baby/child's registered surname (if different)	Surname may change between birth and 42 days (the legal requirement to register the birth)
Baby/child's first name	(First name) to identify the baby
Sex	To identify the baby and to analyse data for difference by gender
Date of birth	To identify the baby and measure performance against KPIs
Gestation of baby at birth	Necessary to interpret baby's screening results
Baby's address line 1	To identify and track baby
Baby's address line 2	As above
Baby's address line 3	As above
Baby's postcode	As above
Ethnic origin	To monitor the disease prevalence by ethnicity and for equality monitoring
Has the baby or child had a blood transfusion?	Necessary to interpret baby's screening results
GP name	To identify and track baby
GP practice code	To identify and track baby
Date of newborn screening test result	To identify the baby and measure performance against KPIs

<b>Data item</b>	<b>Purpose</b>
Newborn screening result	Communicate which condition is suspected
Any other comments on the result	Additional information to clarify result
Mother's NHS number	To improve identification of babies, needed for dataset linkage and quality assurance of linked programme
Mother's surname	As above

Mother's forename	As above
Mother's Hb carrier/affected state	Required to confirm baby's diagnosis in some cases and to evaluate antenatal and newborn linked programme and quality assurance
Father's Hb carrier/affected state	Required to confirm baby's diagnosis in some cases and to evaluate antenatal and newborn linked programme and quality assurance
Prenatal diagnosis (PND) offered/accepted/declined	Evaluate antenatal and newborn linked programme and quality assurance
PND result	Evaluate antenatal and newborn linked programme and quality assurance
Baby/child's hospital number	Unique identifier within an organisation setting
Date NBS results received	To identify the baby and measure performance against KPIs
Date screening result reported to parents	To measure performance against KPIs
Date baby/child attended the haemoglobinopathy medical centre	Confirmation of handover to treatment services and to measure performance against KPIs
Confirmed screening results	Evaluate antenatal and newborn linked programme and quality assurance
Confirmed diagnosis	Evaluate antenatal and newborn linked programme and quality assurance
<b>Data item</b>	<b>Purpose</b>
Date penicillin offered / prescribed/declined (SCD only)	Evaluate antenatal and newborn linked programme and quality assurance
Clinical comments	Additional information to clarify result
Date of death	Evaluate antenatal and newborn linked programme and quality assurance

Cause of death	Evaluate antenatal and newborn linked programme and quality assurance To determine if death can be ascribed to sickle cell disease or thalassaemia
----------------	--

### Data retention:

Based on current legal requirements, professional best practice and user needs, data will be retained until the 25<sup>th</sup> birthday<sup>1</sup>.

<https://digital.nhs.uk/data-and-information/looking-after-information/data-security-andinformationgovernance/codes-of-practice-for-handling-information-in-health-andcare/records-management-code-ofpractice-for-health-and-social-care-2016>

## Sch 3.4 Call-Off Contract Charges

3.4.1. For each individual Statement of Work (SOW), the applicable Call-Off Contract Charges (in accordance with the charging method in the Order Form) will be calculated using all of the following:

- the agreed relevant rates for Supplier staff or facilities, which are inclusive of any applicable expenses and exclusive of VAT and which were submitted to the Buyer during the Further Competition that resulted in the award of this Call-Off Contract.
- the number of days, or pro rata for every part of a day, that Supplier staff or facilities will be actively providing the Services during the term of the SOW.
- a contingency margin of up to 10% applied to the sum calculated on the basis of the above two points, to accommodate any changes to the SOW Deliverables during the term of the SOW (not applicable to Lot 3). The Supplier must obtain prior written approval from the Buyer before applying any contingency margin.

3.4.2 The Supplier will provide a detailed breakdown of rates based on time and materials Charges, inclusive of expenses and exclusive of VAT, with sufficient detail to enable the Buyer to verify the accuracy of the time and material Call-Off Contract Charges incurred.

The detailed breakdown for the provision of Services during the term of the SOW will include (but will not be limited to):

- a role description per Supplier Staff;
- a facilities description;



- the agreed relevant rate per day;
- any expenses charged per day, which are in line with the Buyer's expenses policy (if applicable);
- the number of days, or pro rata for every part day, they will be actively providing the Services during the term of the SOW; and
- the total cost per role/facility

The Supplier will also provide a summary which is to include:

- Total value of this SOW
- Overall Call-Off Contract value
- Remainder of value under overall Call-Off Contract Charge Where:  

$$\text{Remainder of value under overall Call-Off Contract Charge} = \text{overall Call-Off Contract value} - \text{sum of total value of all SOWs invoiced}$$
- Whether there is any risk of exceeding Overall Call-Off Contract value (and thereby requiring a Contract Change Note (CCN) to continue delivery of Services)

3.4.3 If a capped or fixed price has been agreed for a SOW:

- The Supplier will continue at its own cost and expense to provide the Services even where the agreed price has been exceeded; and
- The Buyer will have no obligation or liability to pay for the cost of any Services delivered relating to this order after the agreed price has been exceeded.

3.4.4 Risks or contingencies will be included in the Charges. The Parties agree that the following assumptions, representations, risks and contingencies will apply in relation to the Charges.

Insert full details of any -

Assumptions: None;

Representations: None;

Risks: None and

Contingencies: None

3.4.5 Any changes to the Supplier Staff (not applicable to Lot 3 Services) should be agreed with the Buyer and covered by a separate SOW where it cannot be accommodated within an existing SOW.

3.4.6 Multiple SOWs can operate concurrently.

3.4.7 The Supplier will keep accurate records of the time spent by the Supplier staff in providing the services and will provide records to the Buyer for inspection on request (not applicable to Lot 3 Services)

## Sch 3.5. Call-Off Contract Extension Period

Where the Buyer has specified an Extension Period in the Order Form, the Parties agree that an Extension Period of up to 25% of the initial Call-Off Contract Period can be added to the term of the Call-Off Contract, to accommodate any changes to the Deliverables, or delay in meeting the Buyer's requirements. The Buyer must give the Supplier the minimum notice specified in the Order Form that an Extension Period is required, set out how long the Extension Period is to be,

and obtain prior written approval from the Supplier before applying any Extension Period to the CallOff Contract period.