

Health Systems Support Framework: Template Order Form

Contract Title	Improving Care Coordination for Patients Programme – Technical and Project Support
Order Reference Number	C78061
Date of Order Form	03/08/2022
Authority	NHS Commissioning Board, trading as NHS England, whose principal place of business is Quarry House, Quarry Hill, Leeds LS2 7UE
Suppliers	Carnall Farrar Ltd, [REDACTED]
Principal Supplier(s)	Carnall Farrar Ltd, [REDACTED]
Status of Order Form	Issue of this Order Form is an “invitation to treat” by the Authority following the Suppliers’ Call-Off ITT Response submitted by the Supplier(s) in response to the relevant mini-competition conducted under and in accordance with the Framework Agreement. On the signature of the Order Form by the Suppliers and its return to the Authority, the signature of the Order Form by the Authority shall be the point at which a contract is formed between the Authority and the Suppliers. This Order Form, together with the Call-Off Terms and Conditions and the applicable provisions of the Framework Agreement (and the other provisions as set out in the Call-Off Terms and Conditions) form a contract (defined as “the Contract” in the Call-Off Terms and




	<p>Conditions) between the parties as at and from the date of this Order Form.</p> <p>All terms defined in the Call-Off Terms and Conditions have the same meaning when utilised in this Order Form.</p>	
Call-Off Terms and Conditions	The Call-Off Terms and Conditions comprise the following Schedules of Appendix A of the Framework Agreement:	
	Schedule 1	Key Provisions
	Schedule 2	General Terms and Conditions
	Schedule 3	Definitions and Interpretations Provisions
	Schedule 4	This Order Form
	Schedule 5	Information Governance
	Schedule 6	Security Management
	Schedule 7	Standards
	Schedule 8	Software – Not Used
	Schedule 9	Installation and Commissioning Services – Not Used

	Schedule 10	Maintenance Services – Not Used	
	Schedule 11	Guarantee – Not Used	
	Schedule 12	Staff Transfer – Not Used	
	Schedule 13	Change Control Process	
	Schedule 14	Calculation of Termination Sum – Not Used	
	Schedule 15	Standard License Terms - Not Used	
	Schedule 16	Acceptance Testing – Not Used	
	Any additional Extra Key Provisions set out at Annex 2 below shall be incorporated into the Contract formed by the signature and completion of this Order Form.		
Framework Agreement	The Health Systems Support Framework established by NHS England for and on behalf of NHS England and other contracting authorities and other organisations in relation to the provision of deliverables that may be required for the facilitation and support of sustainable transformation partnerships and/or integrated care systems (the “Framework Agreement”) to which suppliers were appointed following their submission of responses to the framework ITT (“Framework ITT”).		
Call-Off ITT	The Call-Off ITT as issued by the Authority to invite responses to the relevant mini-competition conducted under and in accordance with the Framework Agreement.		

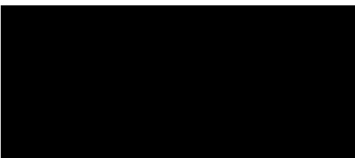
Call-Off ITT Response	The Suppliers' response to the relevant Call-Off ITT submitted by the Suppliers in response to the relevant mini-competition conducted under and in accordance with the Framework Agreement and initiated by the issue of a Call-Off ITT by the Authority.
Term of the Contract	The initial term of the contract is for a 24-month period commencing on the 05/08/2022, with a 12-month extension option.
Extension of Term	The Authority has the right to extend on one or more occasions, up to a maximum of 12 months. If the full extension option is used, this could take the contract to 04/08/2025.
Unilateral Authority right of termination notice period	One (1) Month
Maximum Permitted Profit Margin	N/A – Not Used
Variation to Termination Sum calculation	N/A – Not Used
Deliverables	The Deliverables to be provided by the Supplier(s) under the Contract shall be the Services and/or Ad Hoc Services and/or Goods and/or any other requirement whatsoever (including without limitation any item, feature, material, outcome or output) set out in the agreed work packages throughout the contract period, underpinned by Annex 1 to this Order Form ("the Specification") and shall be provided from the Deliverables Commencement Date set out in the agreed work packages and in accordance with the KPIs set out in the Specification.
Priority Deliverable	This will be identified and agreed in the individual work packages.
Deliverables Commencement Date	As agreed in the Statement of Work packages.

Services Commencement Date	As agreed in the Statement of Work packages.
Goods Commencement Date	N/A – Not Used
Long Stop Date	As agreed in the Statement of Work packages.
Implementation Plan	The implementation plan submitted as part of the Call-Off ITT Response (if required by the relevant mini-competition conducted in accordance with the Call-Off ITT) and set out at Annex 4 below.
Information Security Management Plan	The information security management plan submitted as part of the Call-Off ITT Response (if required by the relevant mini-competition conducted in accordance with the Call-Off ITT) and set out at Annex 5 below, as may be amended from time to time in accordance with Schedule 6 of these Call-Off Terms and Conditions.
Insurance	Insurance levels are as stated in Clause 20 of Schedule 2 (General Terms and Conditions).
Insurance on Expiry or Termination	<p>On the expiry or earlier termination of this Contract, the Suppliers are required to ensure that:</p> <ol style="list-style-type: none"> 1) unless otherwise required in the Extra Key Provisions, any ongoing liability that they have or may have arising out of this Contract shall continue to be the subject of appropriate insurance and/or indemnity arrangements and/or membership of the risk pooling statutory schemes for the period of six (6) years from termination or expiry of this Contract; and 2) where the Deliverables or any part of them could result in liability to any patient in respect of care and/or advice funded by an NHS body, any ongoing liability that the Suppliers have or may have arising out of this Contract shall continue to be

	<p>the subject of appropriate insurance and/or indemnity arrangements and/or membership of the risk pooling statutory schemes for the period of up to twenty-one (21) years from termination or expiry of this Contract.</p> <p>(See Clauses 20.8 and 20.9 of Schedule 2 of the Call-Off Terms and Conditions, respectively)</p>
Key Roles for the supply or performance of the Deliverables and the personnel who will fill those Key Roles (“Key Personnel”)	This will be identified and agreed in the individual work packages.
Premises and Location(s) for the Delivery of the Deliverables	This will be identified and agreed in the individual work packages.
Licence(s) and/or Lease(s) granted to the Suppliers	N/A
Information Governance Provisions (Schedule 5)	The default position under the Call-Off Terms and Conditions is that the Authority shall act as a Controller and the Supplier shall act as a Processor.
Processing of Personal Data	As per Schedule 5 of the Call-Off Terms and Conditions.
Intellectual Property	N/A – No amendments made to Clause 14 of Schedule 2 (General Terms and Conditions)
Supplier Owned Foreground IPR	N/A – All Foreground IPR to be owned by the Authority
Standard Licence Terms	N/A – No amendments made to Clause 15

Acceptance Testing	Not Used				
Contract Price	<p>The price(s) / (Individual Day Rates) to be paid by the Authority to the Suppliers for the provision of the Services, as set out in the Call-Off ITT Response and reproduced at Annex 3.</p> <p>The contract value is up to £10 million. The actual value will depend on the Statement of Work Packages agreed throughout the contract period. The price of the Statement of Work Packages will be based on the submitted Day Rates at Annex 3.</p>				
Financial Model	The Suppliers' Financial Model, submitted if required by the Authority in the Supplier's Call-Off ITT Response and reproduced at Annex 3.				
Contract Price for the purposes of Clause 19 (Limitation of Liability)	Contract price to be agreed for each individual work package.				
Guarantee	N/A – No guarantee required				
Guarantee in favour of NHSE	N/A – No guarantee required				
Payment Provisions	The payment terms for the payment by the Authority to the Suppliers of the Contract Price for the Services, as set out in each agreed work package supported by the submitted day rates at Annex 3.				
Contract Managers	<table border="1"> <tr> <td><i>Authority's Contract Manager</i></td><td></td></tr> <tr> <td><i>Supplier's Contract Manager(s)</i></td><td></td></tr> </table>	<i>Authority's Contract Manager</i>		<i>Supplier's Contract Manager(s)</i>	
<i>Authority's Contract Manager</i>					
<i>Supplier's Contract Manager(s)</i>					

Lead Contract Manager (if applicable)	<p><i>Insert the Lead Contract Manager at the commencement of this Contract</i></p> <table border="1" data-bbox="587 383 1324 488"> <tr> <td data-bbox="587 383 954 488"><i>Supplier's Lead Contract Manager</i></td><td data-bbox="954 383 1324 488"></td></tr> </table>	<i>Supplier's Lead Contract Manager</i>	
<i>Supplier's Lead Contract Manager</i>			
Contract Meetings	Meeting frequency to be agreed by both the Authority and Supplier in each individual work package. The Authority will minute each meeting in accordance with Clause 11 of Schedule 2 of the Call-Off Terms and Conditions.		
Fast-track Change values	N/A		
Contract Reports – additional information	As per Clause 11.3 of Schedule 2 of the Call-Off Terms and Conditions.		

Name:	[REDACTED]	Position:	Chief Financial Officer
Signed by the authorised representative of the AUTHORITY  Full Name: [REDACTED] Job Title/Role: Chief Financial Officer, NHS England Date Signed: 16/08/2022			

Name:	[REDACTED]	Position:	Head of Business Development
Signed by the authorised representative of the Supplier  Full Name: [REDACTED] Job Title/Role: Head of Business Development Date Signed: 03/08/22			

Order Form Annexes

Annex 1

Part 1: Specification

Part 2: KPI Overview

Part 3: KPIs

Part 4: Calculation of Service Credits

Part 5: Termination Trigger for Accrued KPI Failures

Part 6: Excusing Events

Annex 2

Extra Key Provisions

Annex 3

Contract Price and Payment Terms

Maximum Payments on Unilateral Termination

Supplier's Financial Model

Annex 4

Implementation Plan

Annex 5

Information Security Management Plan

Annex 6

Supplier Solution

Annex 1

Annex 1 Part 1: Specification

Background and Introduction

The NHS EI Office of Chief Data & Analytics Officer was established to provide system wide leadership for analytics and informatic programmes across the NHS. This includes supporting the NHS to deliver better health and care to citizens and patients through the use of data and analysis.

In 2020, the NHS made a strategic decision to establish NHS Data Platform. The NHS Data Platform has proved a valuable resource in the work to support the NHS to meet the challenges in managing the Covid 19 incident as well as respond to the needs of multiple needs including vaccinations.

The NHS is now moving from managing the Covid 19 incident into a mode of managing the consequences of the incident on the NHS and specifically managing the recovery of elective services. The Improving Elective Care Coordination for Patients Programme [ICCPP] seeks to support elective care recovery through the application of the powerful tools inherent in the NHS Data Platform. The IECCPP will achieve this by rolling out the Proof of Concept [POC] NHS Trust Waiting List Management solution, theatre scheduling system and ICS Care Coordination Centre to support up to thirty trusts in their recovery. This Waiting List Management POC was first piloted at Chelsea and Westminster Hospital Trust as a module operating within the NHS Data Platform.

The technical capabilities and support needs of each of up to 30 trusts taking part in this Pilot Programme will be different depending on a range of factors, including what the electronic patient record [EPR] system is deployed.

We are looking to procure a service to deliver support as the Prime Contractor who will provide a range of service capabilities [as defined in the specification TBC] to support the trusts deploying the NHS Trust Waiting List and ICS Care Coordination Centre module.

We are looking to set up a call off contract with a Prime Contractor of up to £10,000,000 (excl VAT) to support this work.

Standards and Service Specifications

For this project, the supplier must be ready to provide robust technical skills paired with deep knowledge of the NHS across national, regional and local levels. This is imperative to improve to help deploy the CCS solution at a pace that will meet the challenging timescales of this programme.

The selected supplier will be expected to be able to act as a Prime Contractor able to provide sufficient of the following types of resources either through consortium or teaming arrangement:

- 1) Service Desk provision at a Trust level to provide Level 1 support
- 2) Data Quality support to help clean and reduce the waiting list data
- 3) Technical Delivery management of the rollout at Trust
- 4) Operational Delivery of digital change and training to staff at the Trusts
- 5) Trainers to deliver training to users in the Trust

5) Service Desk Analysts

We estimate the immediate duration of need for these services to be up to 12 months, but with immediate high demand in the first 2 to 3 months This service shall provide the following:

- Responsibilities: First point of contact for Trust users, handling phone enquiries and raising IT tickets for further investigation by other teams.
- Skills: Experience of managing a service desk.
- Service Availability: Initial Triage and Technical Support available - Mon-Fri, excluding bank holidays and weekends. Business Days in accordance with Greenwich Mean Time (GMT).

5) Data Quality Analyst Support

We estimate the immediate duration of need for this service to be 4 months. This service shall have the following:

- Responsibilities:
 - Work with Palantir to clean data ready for ingestion into the solution
 - Provide data quality advice and guidance to other colleagues in the Trusts
 - Feedback changes that will need to be made to data management within trusts.
- Skills Required:
 - Experience of data quality activities
 - Understanding of NHS data
- Key deliverables:
 - Baselined data [Technical Onboarding]
 - Ongoing data quality management [BAU]

5) Technical Delivery Management

We estimate the immediate duration of need for this service to be 4 months This service shall have the following:

- Responsibilities:
 - Have operational responsibility for delivery of the solution into Trust
 - Act as the first point of contact to ensure the roll out at the Trust runs smoothly and efficiently
 - Develop and maintain good working relationships within the Regional Delivery Manager and staff within the Trusts
 - Monitor performance, activity and other project relevant information such as Funding

- Skills Required:
 - Experience of managing complex processes
 - Experience of delivering change within the NHS
 - Experience of managing technical IT implementation
- Key deliverables:
 - Technical Assessment (*Initial Launch*)
 - Local approval document(s) (*Local Planning*)
 - Resource plan and Funding requests (*Local Planning*)
 - Change management plan and collateral (*Local Planning/Technical Onboarding*)
 - Specialty training and rollout plan (*Technical Onboarding*)
 - Progress report (*Hypercare*)

5) Operational Delivery

We estimate the immediate duration of need for this service to be 2 months. This service shall have the following:

- Responsibilities:
 - Train Clinical, Operational and Administrative staff to use the solution
 - Support the change at a Trust level, including sharing the solution in meetings, demos and 1-2-1 sessions
 - Responsible for adoption in chosen specialty
 - Provide feedback and data for monitoring of progress, activity and other relevant information
- Skills Required:
 - Experience of delivering change within the NHS
- Key deliverables:
 - Training in chosen specialty (*Hypercare*)

5) Operational Delivery

We estimate the immediate duration of need for this service to be 4 months. This service shall have the following:

- Responsibilities:
 - To be a source of advice and knowledge on education and training matters to clinical staff and managers
 - Develop and deliver training to the deployment teams so they can train locally within the Trust
- Skills Required:
 - Evidence of working within professional multi-disciplinary team
 - Experience of training users in a digital system
 - Good understanding of digital systems
- Key deliverables:
 - Training across specialties (*Technical onboarding/Hypercare*)

Essential Skills

The following are the essential skills and experience required from the supplier for them to successfully deliver this:

Resources

- Resources available and of sufficient breadth to meet the needs outlined in the standards and service specifications as defined within this specification
- Ability to act as a Prime Contractor and with a network sufficient to meet the resource requirements through consortium or teaming arrangement as defined within this specification.

In addition the Prime Contractor organisation should meet the following:

Technical Skills and Experience

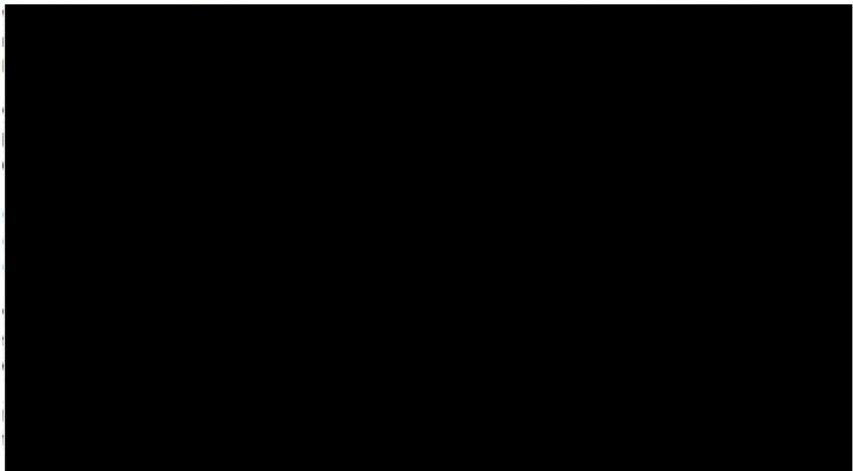
- Ability to develop and deploy tools in Palantir's Foundry platform
- Demonstrated track record of successfully deploying and maintaining tools for national, regional and local healthcare organisations, both in and out of the Foundry platform
- Demonstrated track record of designing and launching effective capability programmes focused on analytics
- Deep understanding of and direct experience working with NHS England, including how it manages planning and delivery
- Experience working with the NHS England nationally as well as at the ICS/STP and provider levels
- Strong problem solving ability for both technical and non-technical applications, with robust systems, methodologies, tools and protocols in place
- PMO / Agile skills in analytics product delivery environment
- Excellent knowledge of the integrated planning tool environment or similar
- Analytical product delivery, performance and management experience

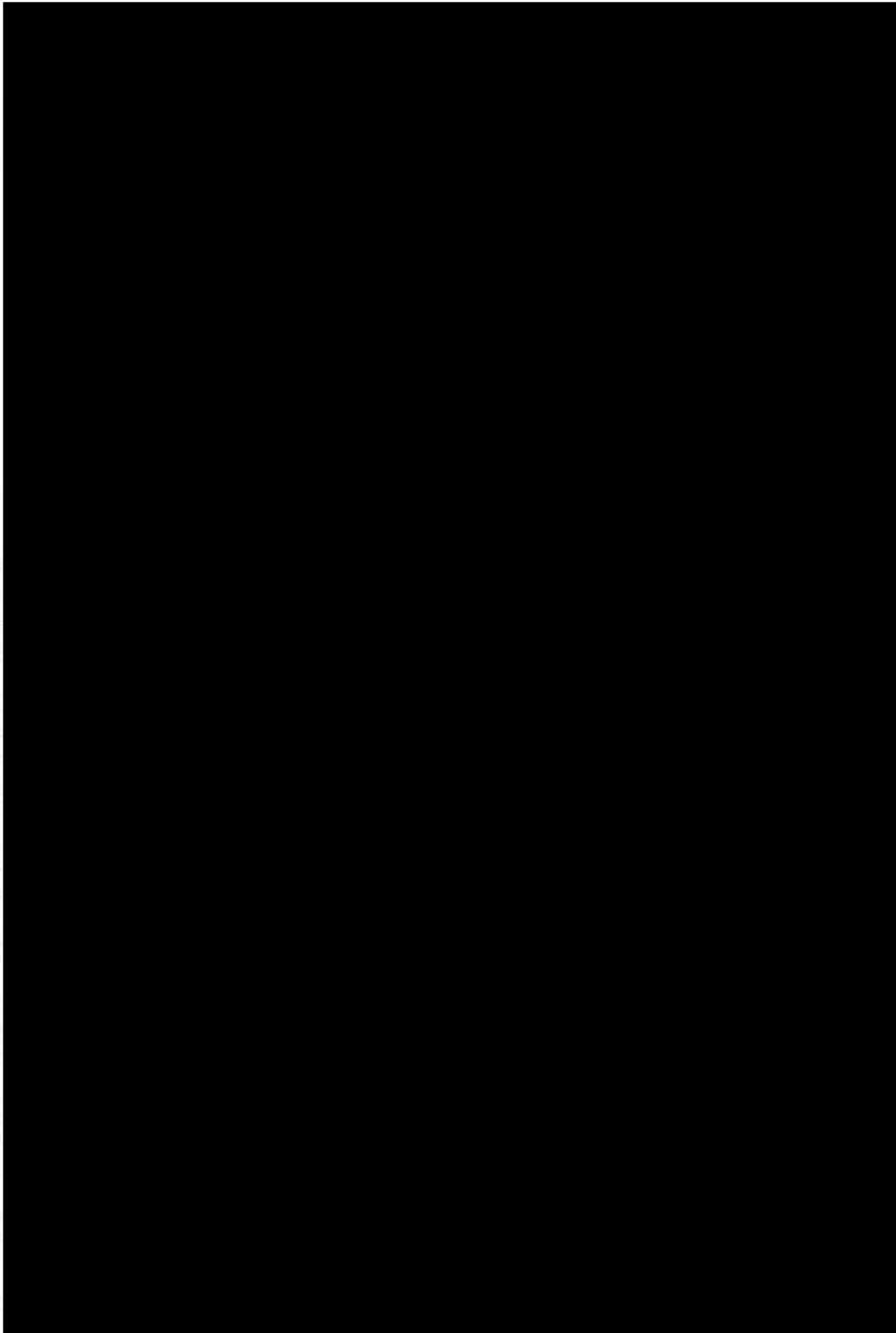
Carnall Farrar – Call Off ITT Response

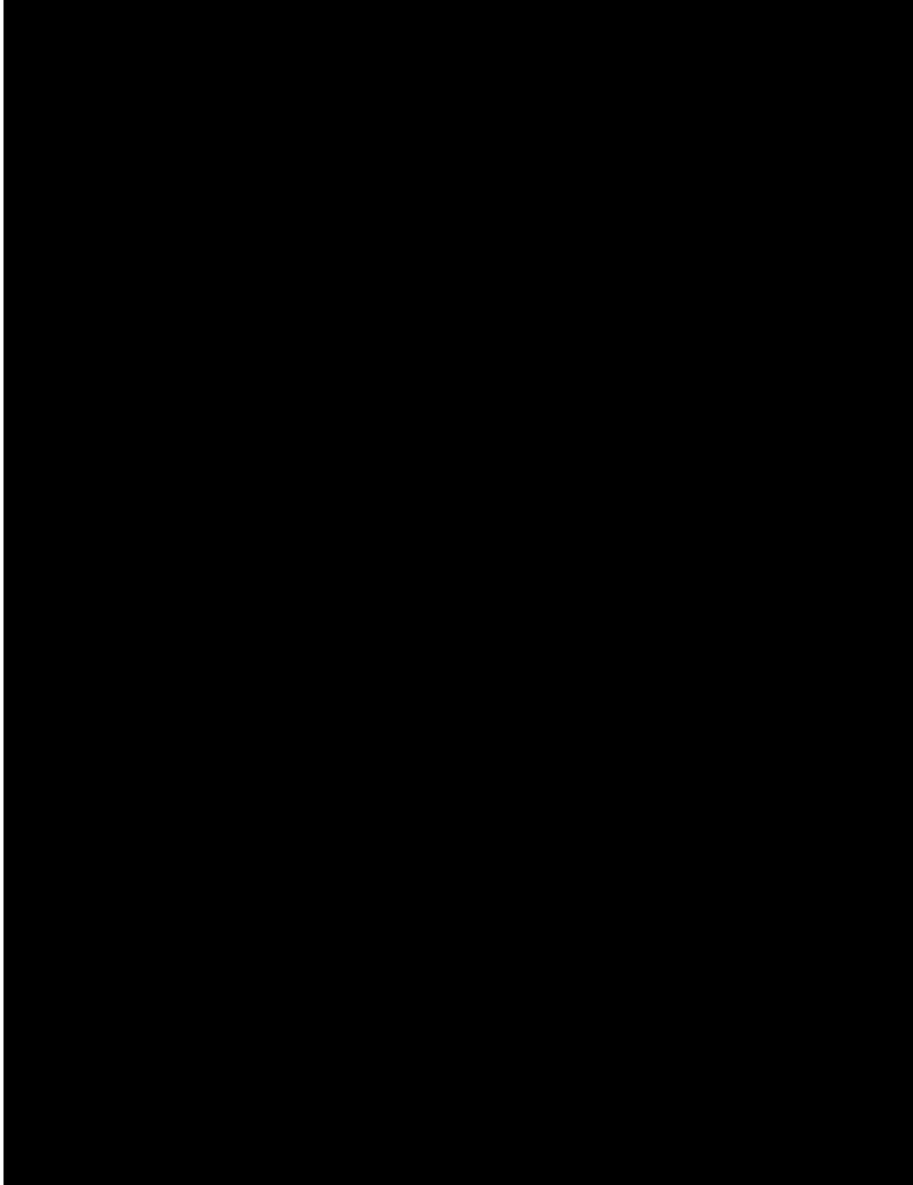
Question 1. Supplier delivery method and assurance criteria against needs of a large-scale programme of work

Weighting: 7.5%	Word Limit 1000 words
<p>Please describe your approach to delivery and governance wrapper [including adssurance criterias and processes] that will be used to assure delivery of a large scale programme of work similar to the Improving care coordination for Patients Programme [ICCPP] Proof of Concept.</p> <p>Please also propose how you would undertake and deliver the requirements of this programme of work.</p>	

Our Approach to Delivery and Governance







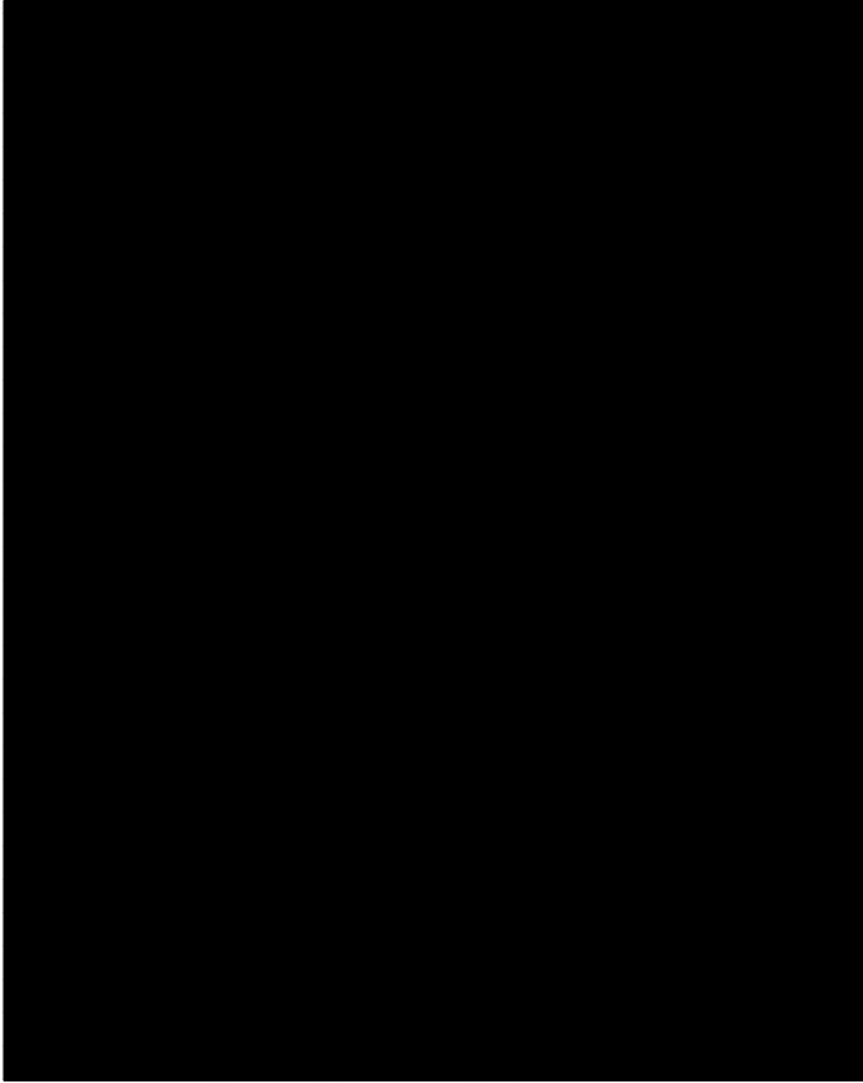


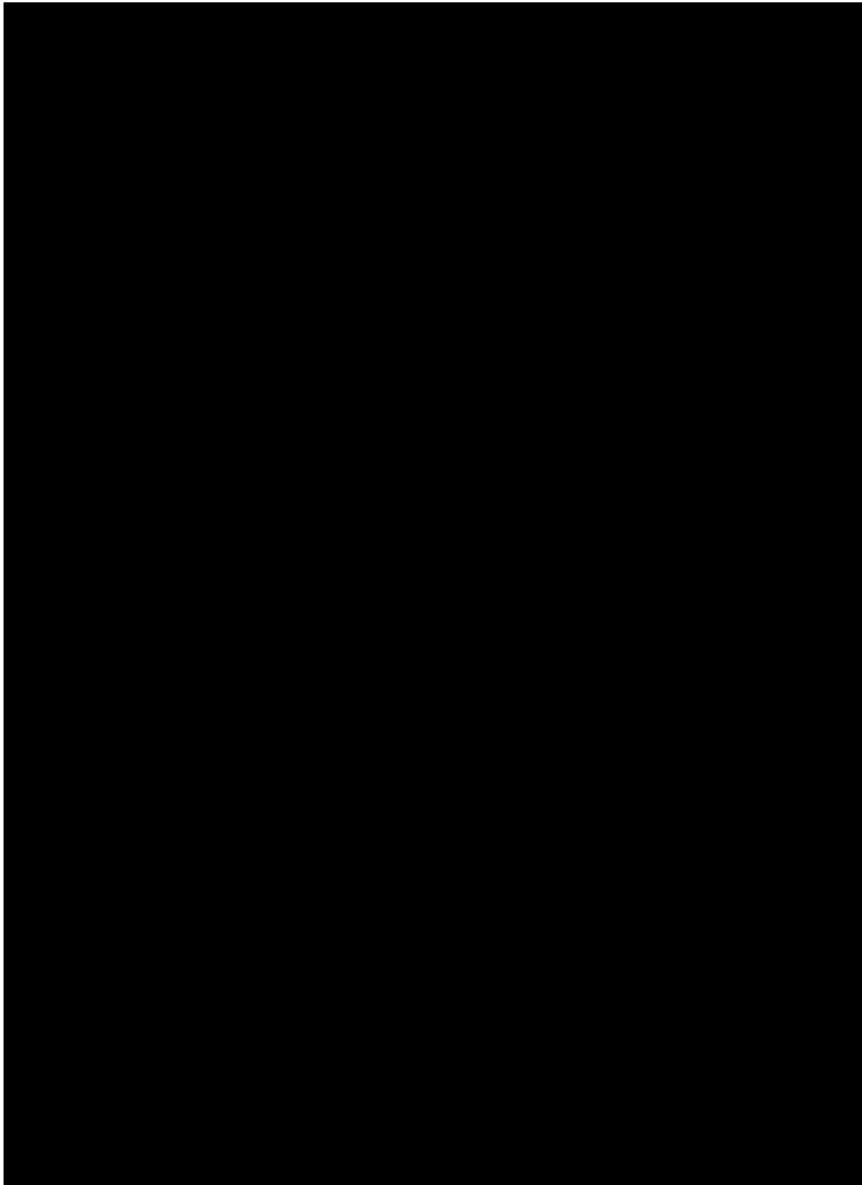
CF | Response to Call-off ITT for ICCPP Bid

5

Question 2. Supplier delivery capability and approach to deployment to meet the needs of the Improving care coordination of Patients Programme [ICCP] Proof of concept.

Weighting: 5%	Word Limit 1000 words
Please describe your delivery capability and how you would deploy that capability to support delivery on our current plans. In particular please describe your delivery (local, near shore and off-shore) capabilities / resources.	





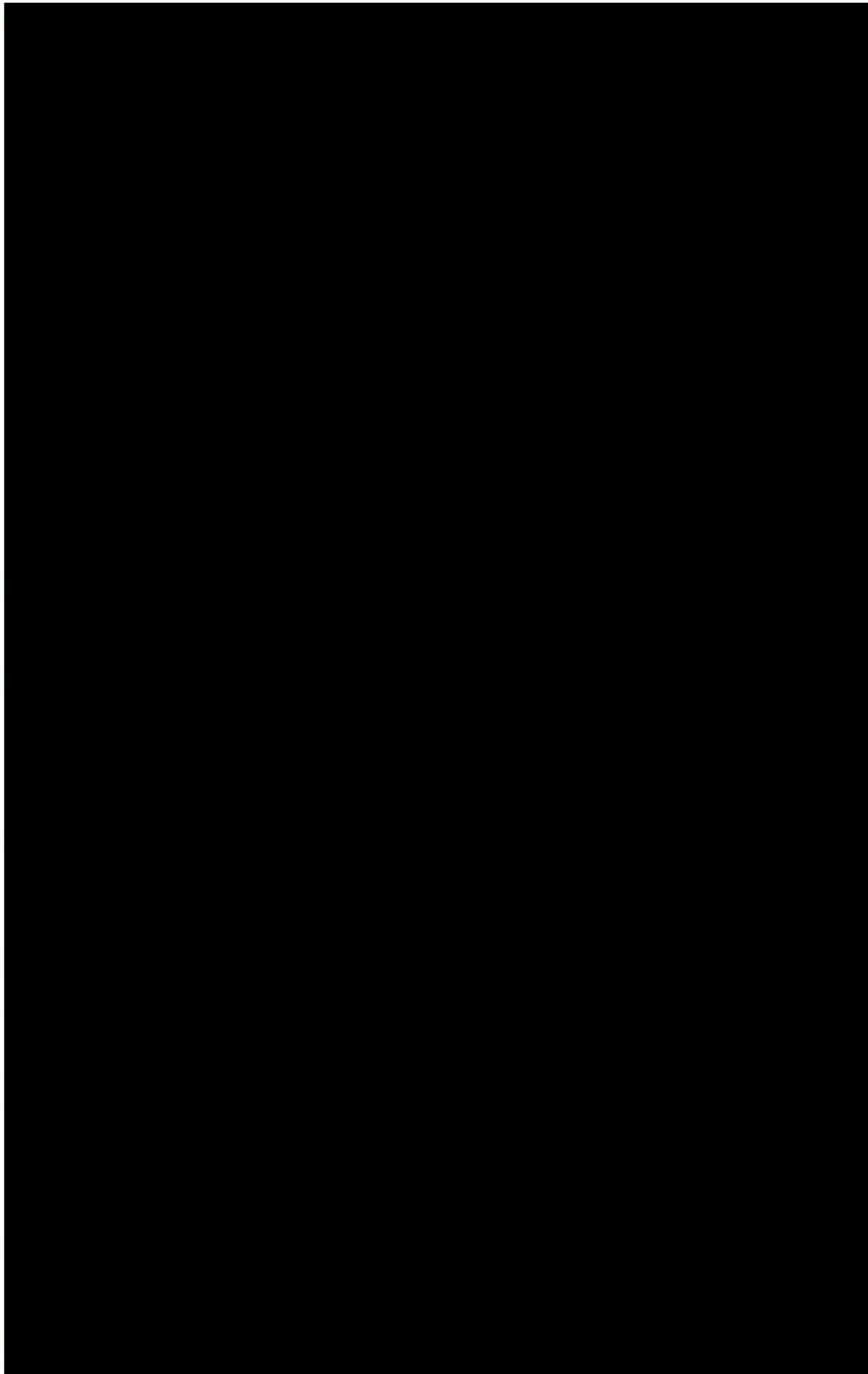
CF | Response to Call-off ITT for ICCPP Bid

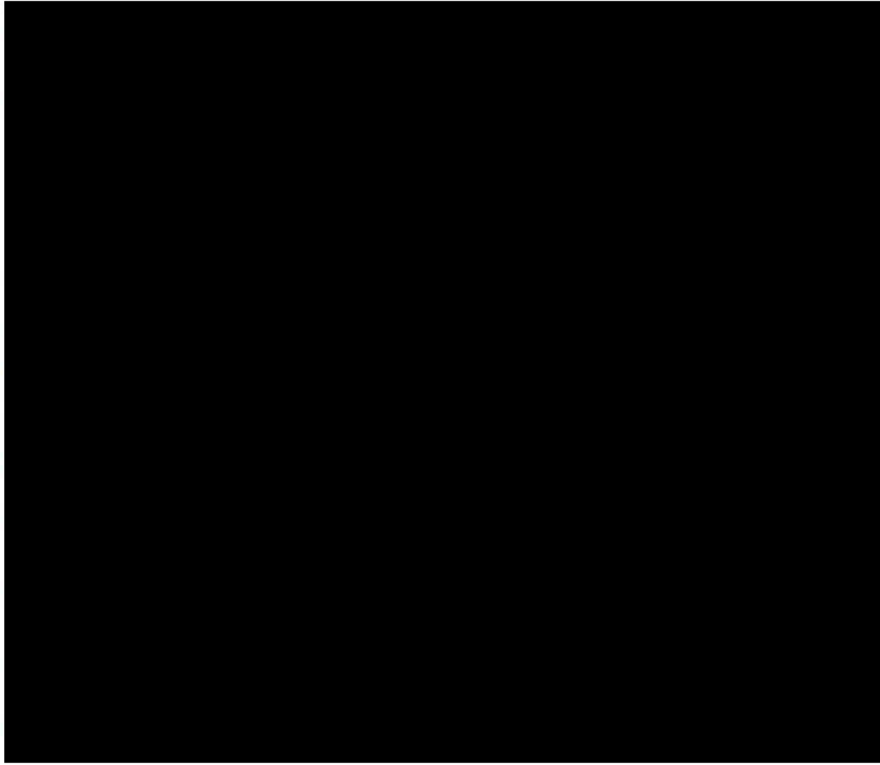
8



Question 3. Experience in delivering transformational change involving partnership within the NHS, and multiple stakeholders

Weighting: 7.5%	Word Limit 1000 words
Please describe your partnership approach on supporting us achieving our ambition. Please give examples of successful partnerships similar to the [ICCPP Proof of Concept] including multiple organisations, stakeholders and workforce including transformational changes.	

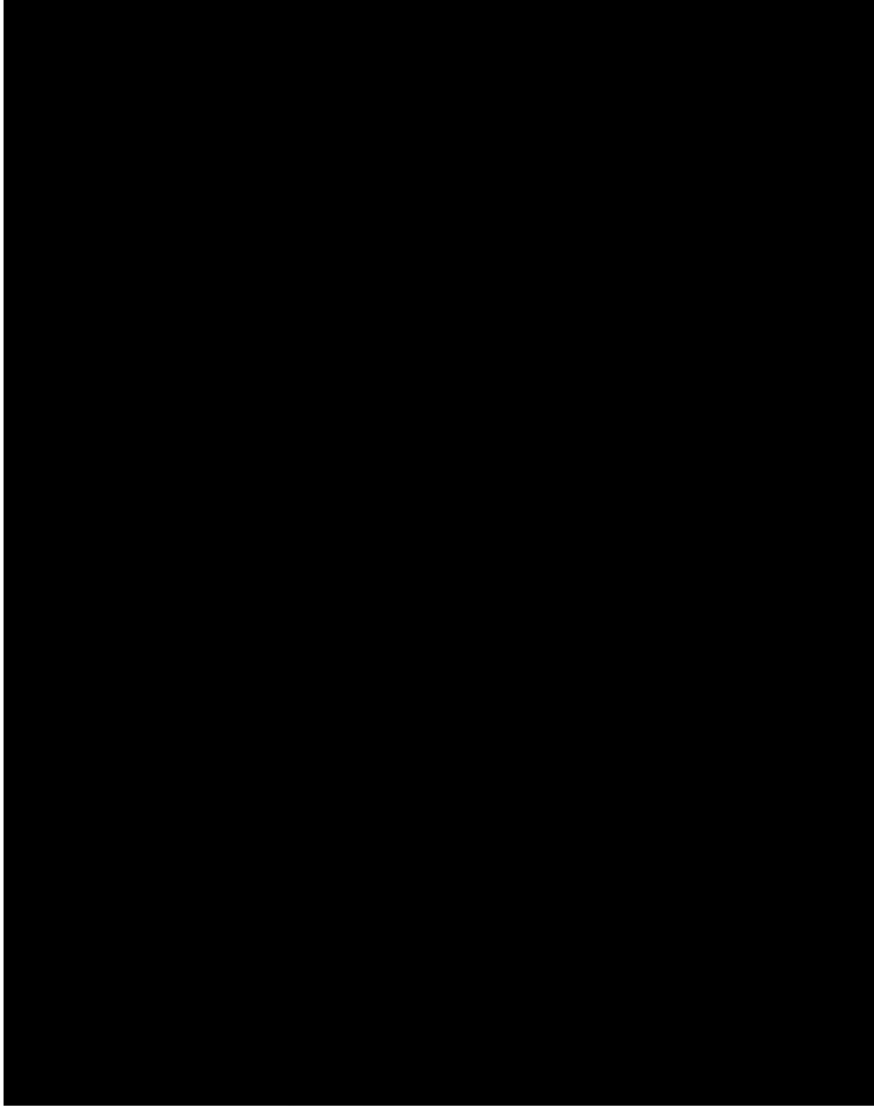


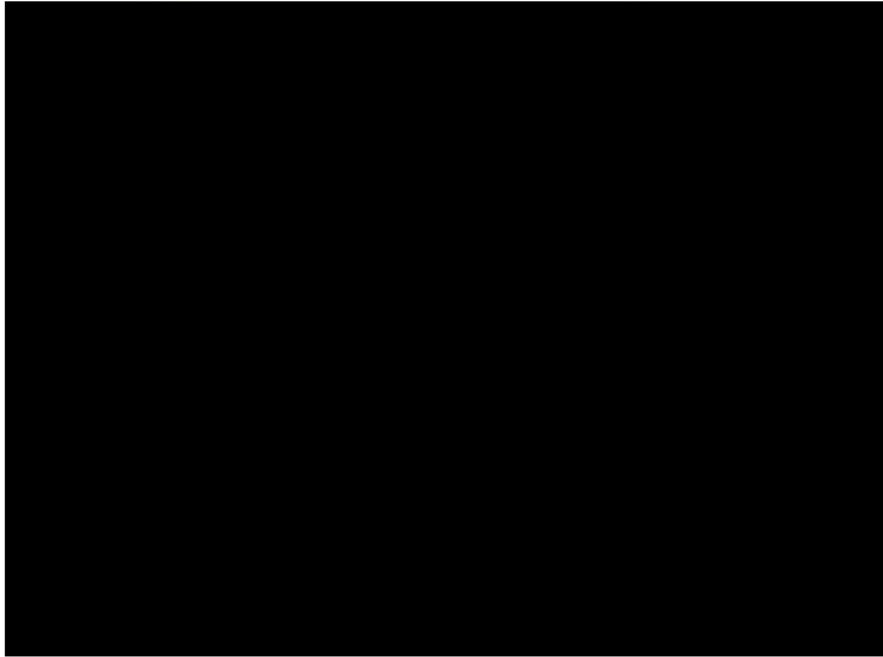


Word Count:971

Question 4. Experience of acting as prime contractor and managing 3rd suppliers

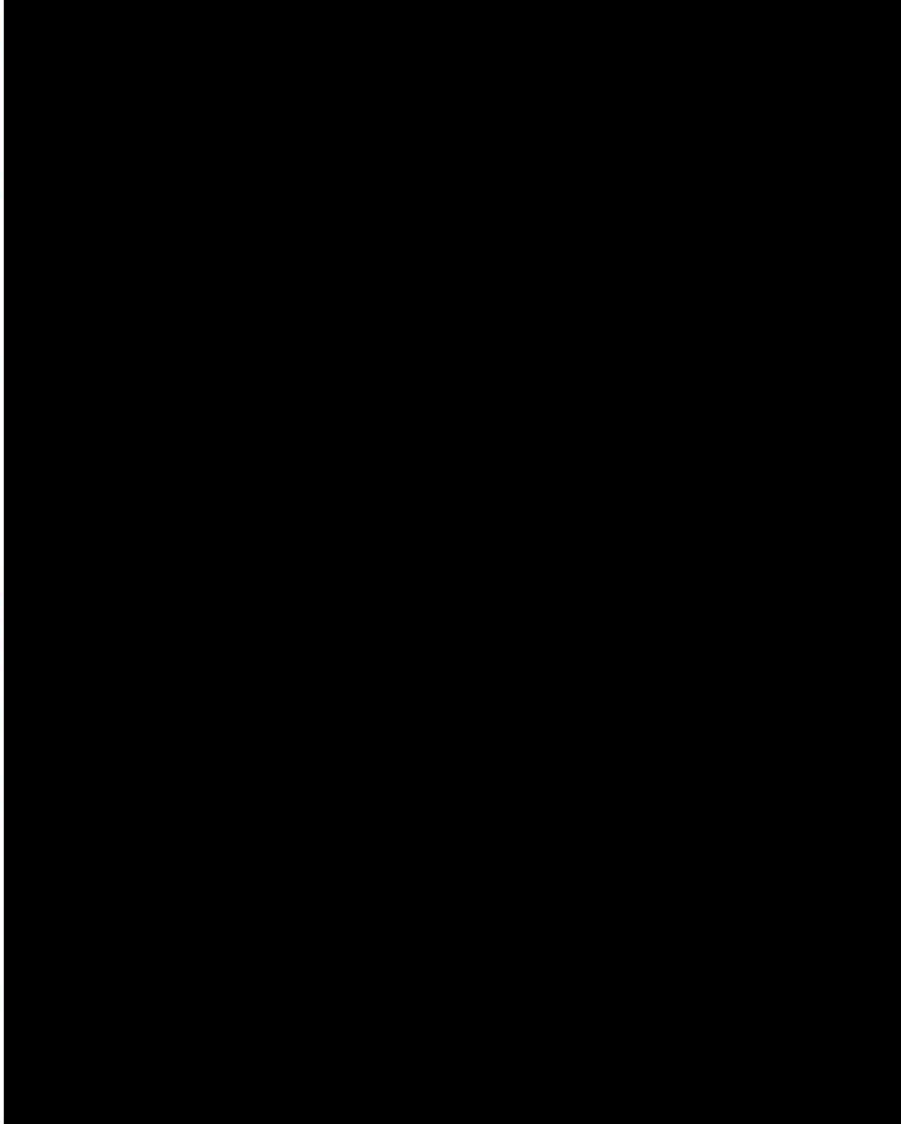
Weighting: 7.5%	Word Limit 1000 words
Please demonstrate your experience as a prime contractor of services and of successfully working within such constraints including multiple 3rd party suppliers / solution providers and dealing with complexity of delivery solutions in tight timescales.	

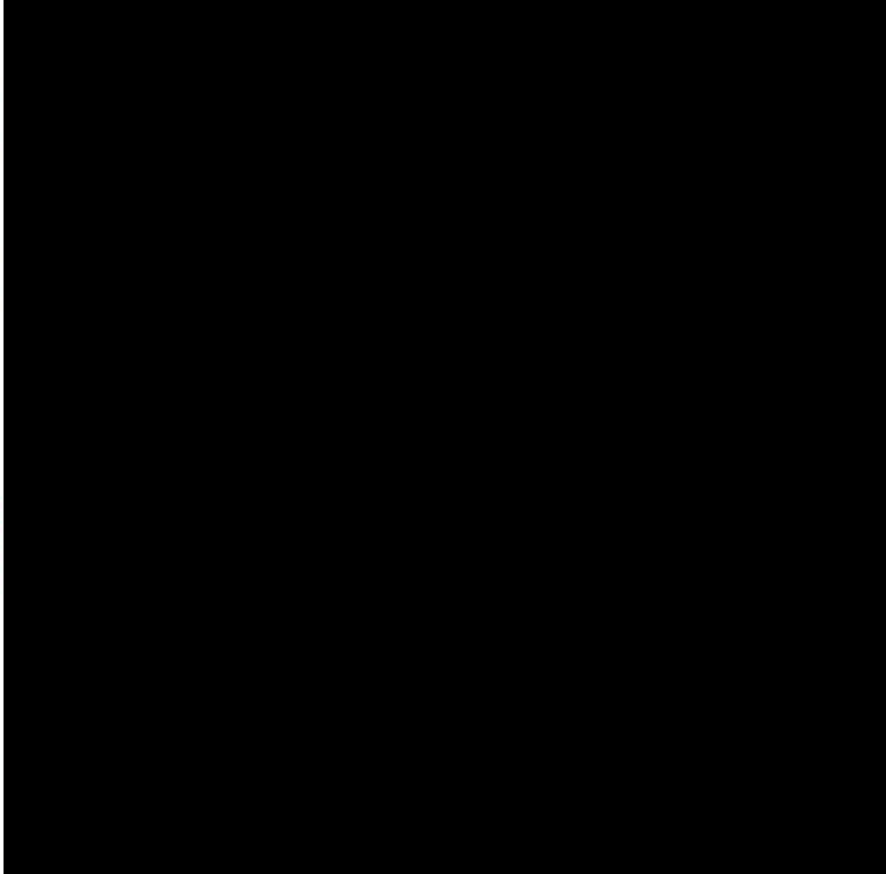




Question 5. Delivery of requirements to industry standards of programme management

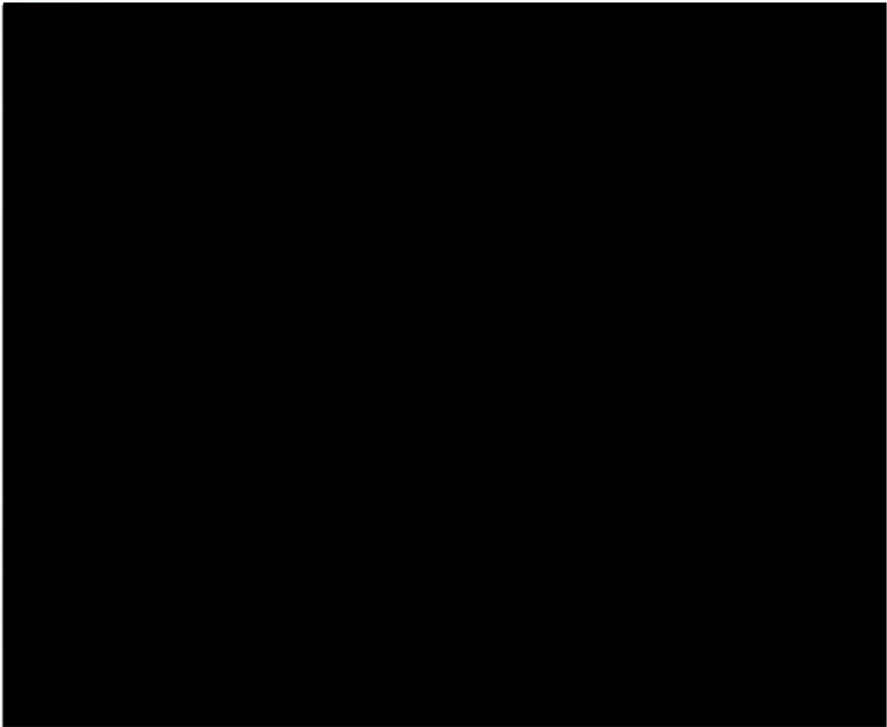
Weighting: 5%	Word Limit 1000 words
Please describe how you will deliver the requirements of this Schedule to industry standard program / project and quality management methodologies.	

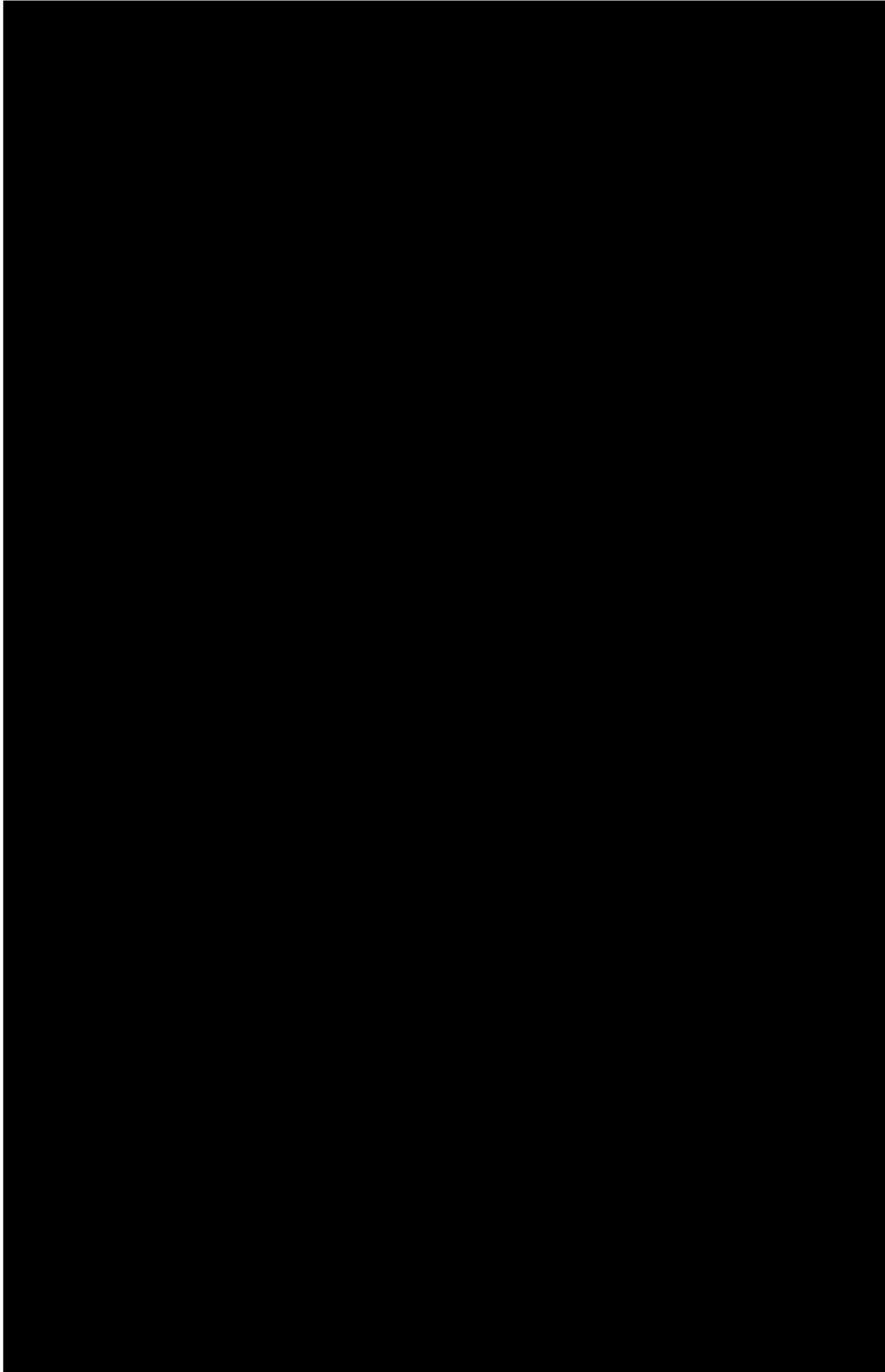


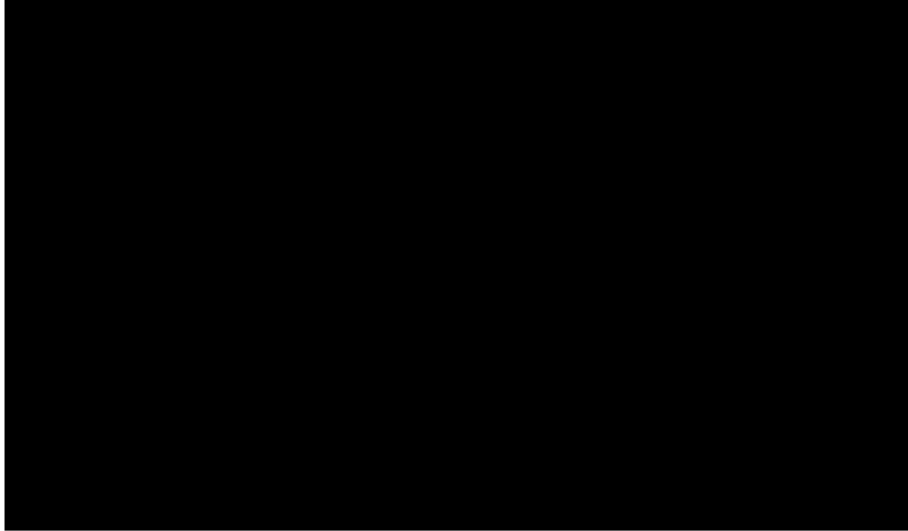


Question 6. Supplier ability to mobilise resources at pace and to share knowledge with customers

Weighting: 7.5%	Word Limit 1000 words
How do you ensure you can mobilise capability and capacity rapidly and effectively, including how you can ramp up and ramp down as required. How do you ensure continuous development and upskilling of our staff and highlight any investments you make in this space?	

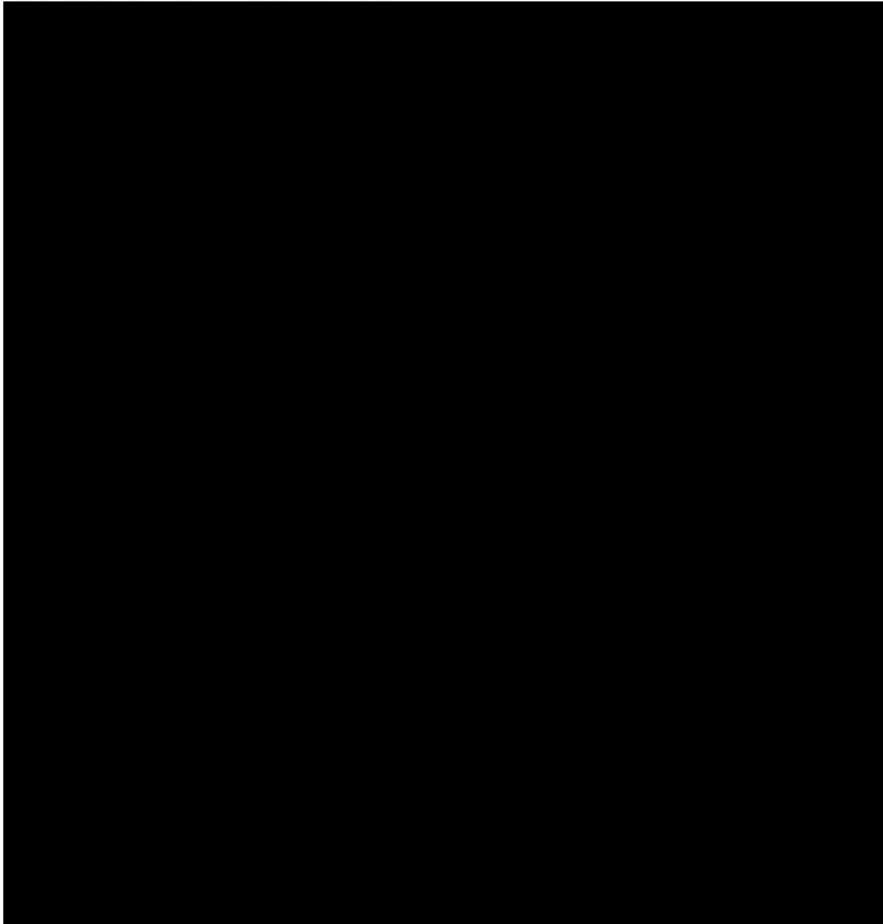


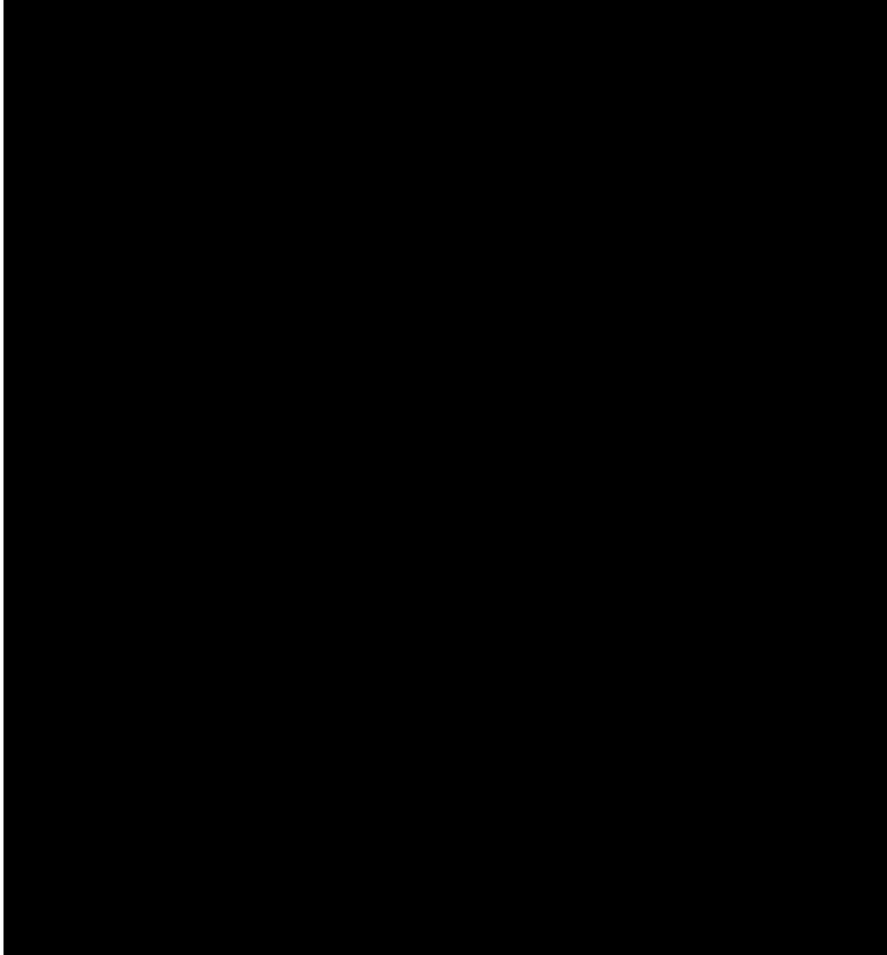




Question 7. Supplier approach to deploying and assuring deployment of third-party products

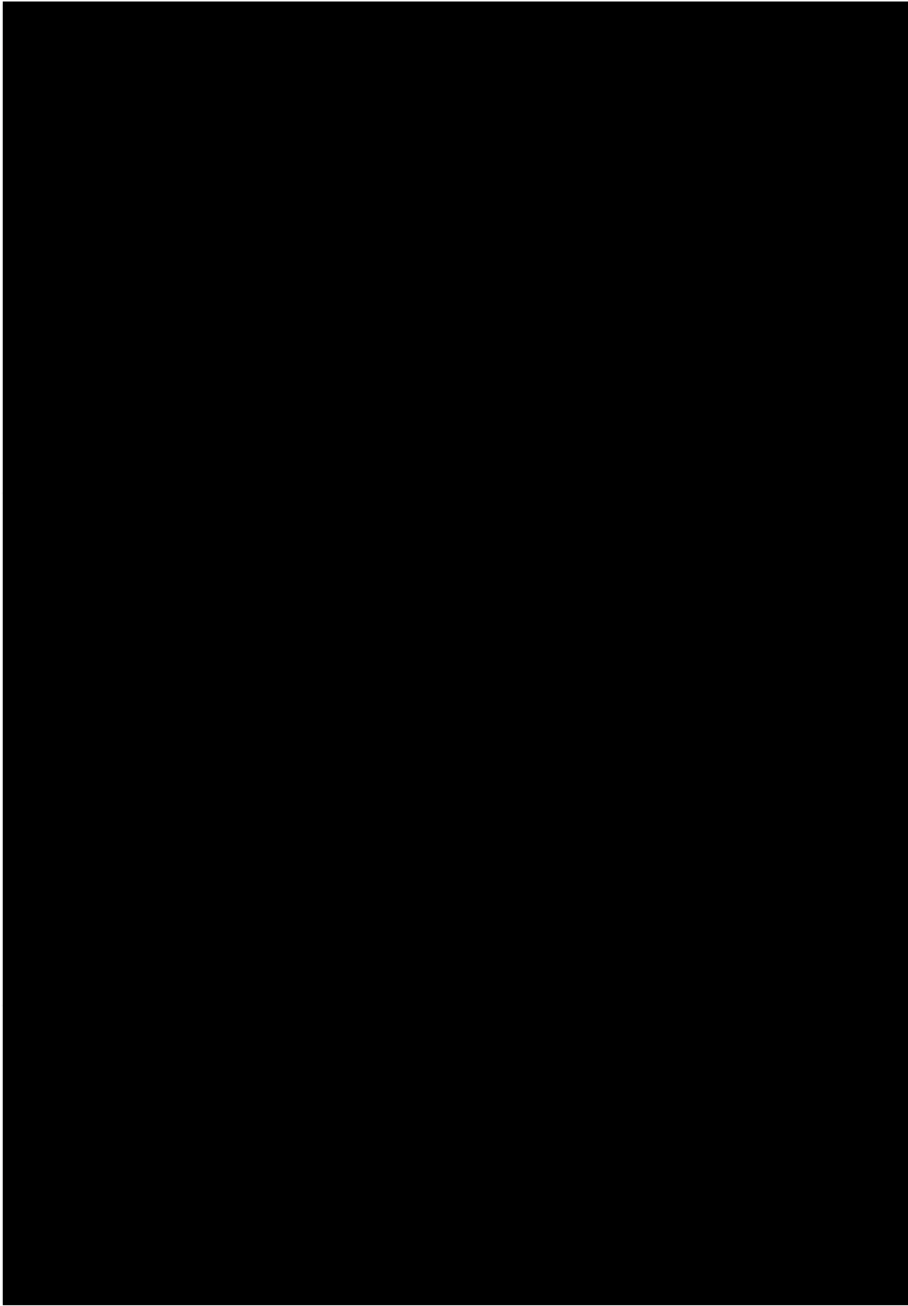
Weighting: 5%	Word Limit 1000 words
Please describe how your approach ensures that any solutions / systems are deliverable and operable for end users in healthcare. Demonstrating careful consideration of the recommendation, configuration and deployment of 3rd party products meeting performance requirements.	

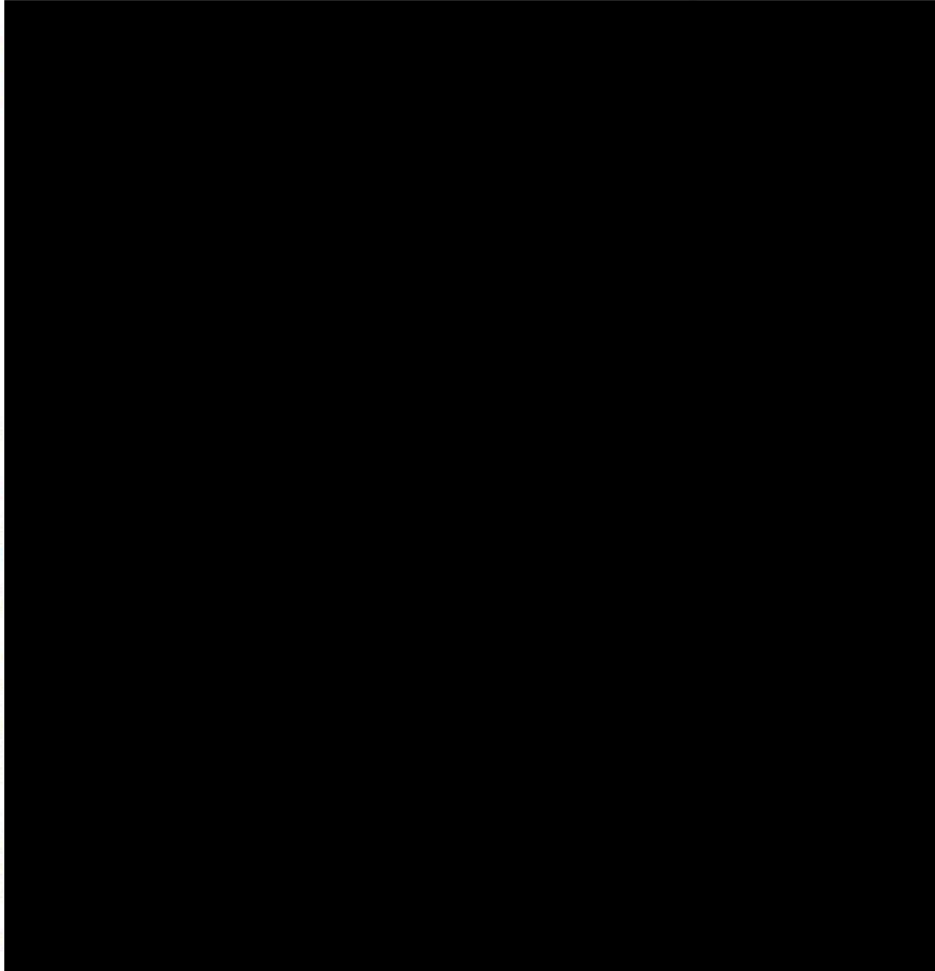




Question 8. Approach to change management when deploying new solutions

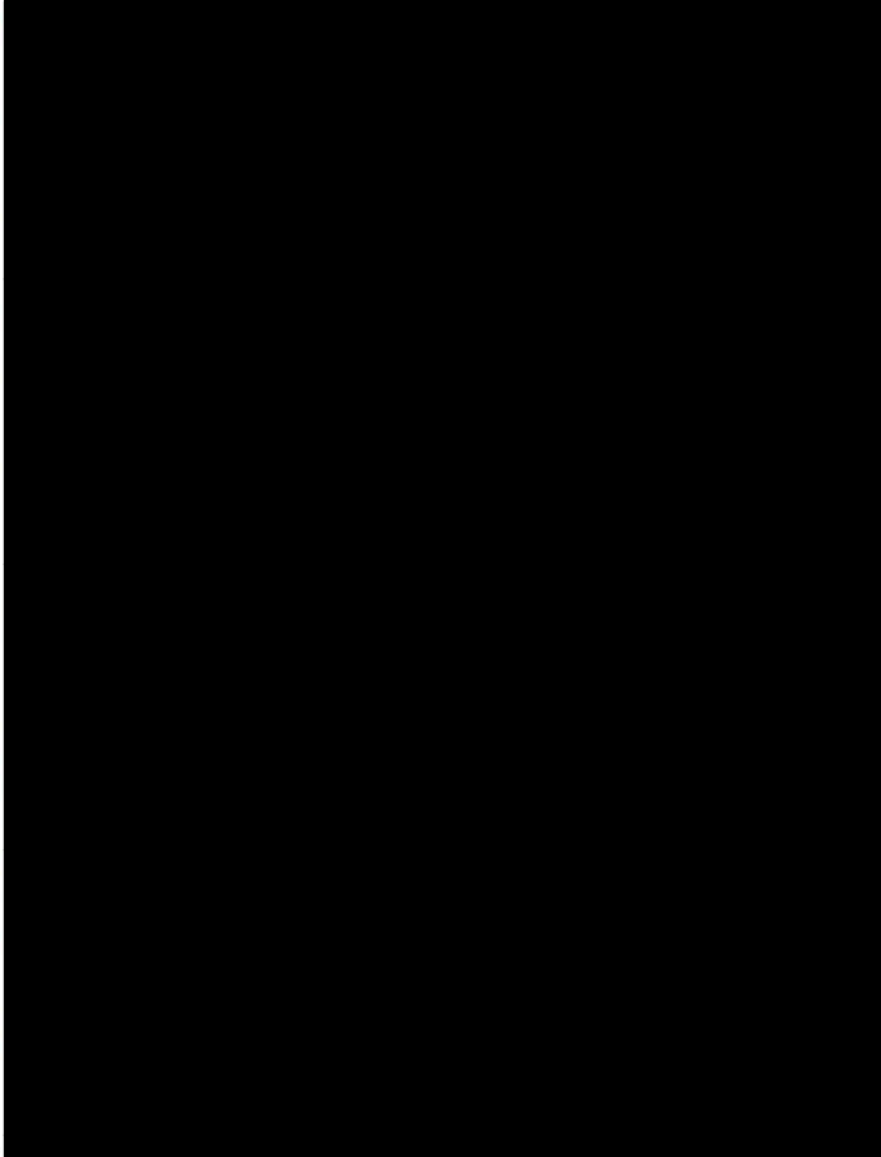
Weighting: 5%	Word Limit 1000 words
Please describe your approach and toolset for change management when supporting the deployment of new solutions or new ways of working.	





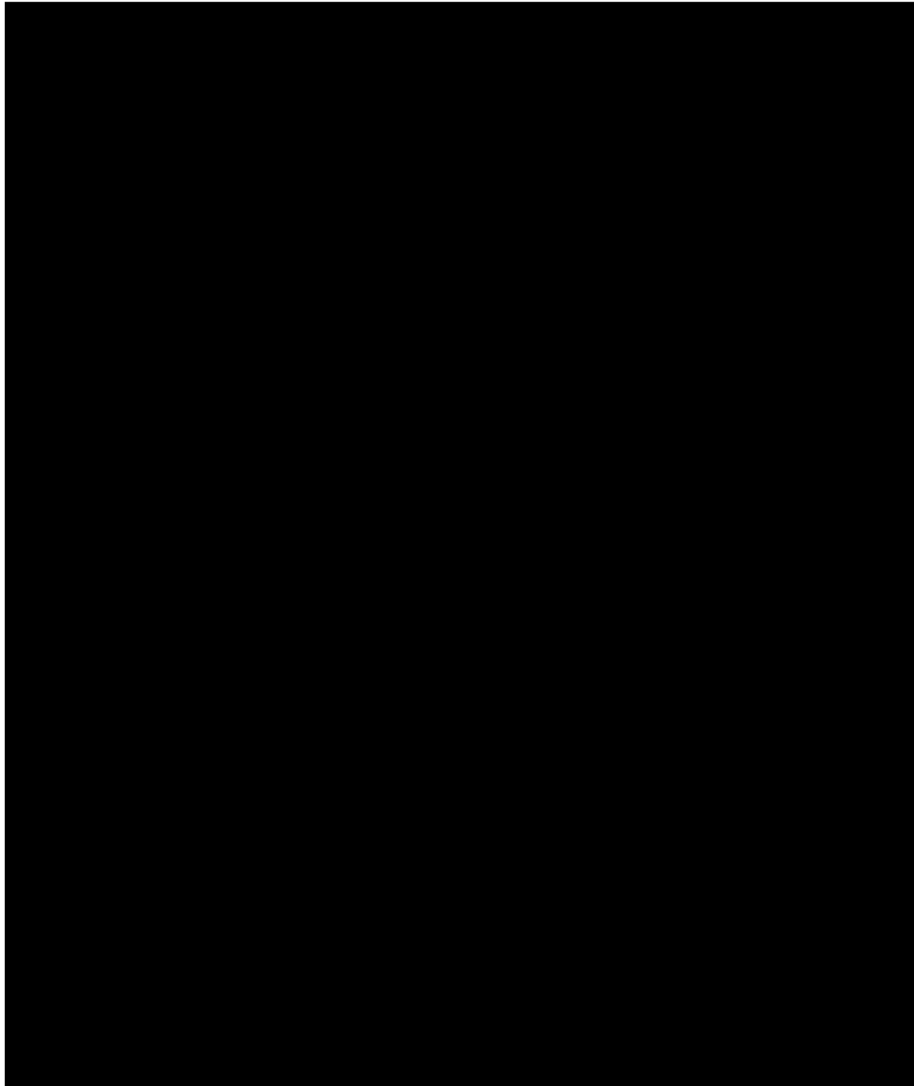
Question 9. Social Value

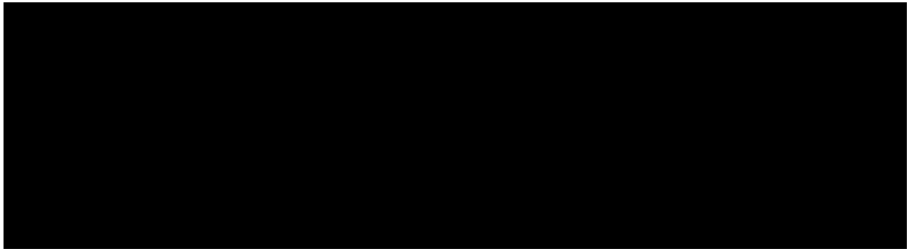
Weighting 2.5%	Word Limit 750 words
Please describe how your organisation would recruit, retain and support employees and other partners engaged in the performance of this contract and how you would monitor and measure this.	



Question 10. Equality and Inclusion

Weighting 7.5%	Word Limit 750 words
Please describe how you will deliver the contract in a way that ensures compliance with labour rights and ethical issues and generates social value out of the health pound. In your response you should highlight how you have demonstrated this and provided work life balance for you team.	





Annex 1 Part 2: KPI Overview

Key Performance Indicators

Not used. To be agreed in the individual work packages.

Annex 1 Part 3: KPIs

Not used. To be agreed in the individual work packages.

Annex 2
Extra Key Provisions

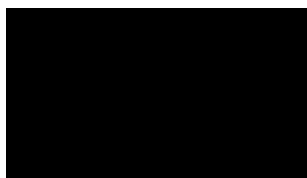
Not used.

Annex 3

Contract Price and Payment Terms

Call-Off Contract Charges and payment	
Contract Price	As agreed in each Statement of Work Package
The method of payment for the Call-Off Contract Charges (GPC or BACS)	BACS
Invoice (including Electronic Invoice) details	http://www.tradeshift.com/supplier/nhs-sbs/
Who and where to send invoices to:	Invoices containing the NHSE Purchase Order Number or Reference Number, and addressed to NHS England, Phoenix House, Topcliffe Lane, Wakefield, WF3 1WE should be submitted via Tradeshift: http://www.tradeshift.com/supplier/nhs-sbs/
Invoice information required	Buyers Purchase Order Number Contract Reference Description of Services
Invoice frequency	As agreed in each Statement of Work Package

The Carnall Farrar submitted Pricing Schedule is attached below:



The Carnall Farrar submitted Day Rates (as shown below) shall be used to calculate the pricing for all Statement of Work Packages throughout the contract period.

	ROLE	Improving Care Coordination For Patients Programme Day Rate	Improving Care Coordination For Patients Programme Hourly Rate
1	Senior Partner		
2	Partner		
3	Associate Partner/Junior Partner		
4	IT Specialist/Consultant		
5	Project Manager (large 50+ people and/or complex)		
6	Data Modellers		
7	Systems Analyst		
8	Senior Programmer/Senior Tester		
9	Analyst Programmer/System Programmer		
10	Programmer/Tester		
11	Database Administrator/Designer and Database Dev		
12	Quality Assurance Analyst		
13	Senior Business Analyst/Senior Designer		
14	Business Analyst/Analyst Designer		
15	LAN Support		
16	Project Administrator		
17	Data Network Designer/Engineer (WAN) N/A		
18	Capacity Planner/System Tune		
19	IT Strategy Planners		
20	Program Manager		
21	Training Lead		
22	Training Associate		
23	Change/ Release / Configuration Manager		
Please input additional roles your organisation are able to provide within the scope of this ITT.			
	ROLE	Improving Care Coordination For Patients Programme Day Rate	Improving Care Coordination For Patients Programme Hourly Rate
1	Service Desk Team Lead		
2	IG Consultant		
3	Senior Programme Manager		
4	Principal Developer		

Annex 4

Implementation Plan (if any)

As per Carnall Farrar's submitted technical response, attached below:



Annex 5

Information Security Management Plan

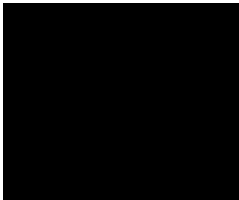
NHSE Information Security Policy



Information
Security Policy v1.0.c

Annex 6

Supplier Solution



Annex 7

Processing of Personal Data

NOTE THE CONTRACT IS TO BE SIGNED, WITH THE CONDITION OF ANNEX 7 BEING REVIEWED, AGREED, AND FINALISED AFTER CONTRACT SIGNATURE. THIS HAS BEEN AGREED VIA EMAIL BETWEEN JOEL LEVER (HEAD OF BUSINESS DEVELOPMENT AT CF) AND JAKE SMITH (SENIOR PROCUREMENT MANAGER AT NHSE).

Operational working policies

- CF nor our sub-contractors will have access to an admin account and we won't be able to alter this access right
- CF nor our sub-contractors will be responsible for revoking access
- CF nor our sub-contractors should be able to download directly identifiable information and we agree no one will attempt to
- No clinical decisions will be made by CF or our sub-contractors with access to the data
- CF and our sub-contractors will only review trust clinical systems whilst sitting next to someone from the trust information team and comparisons will be made on screen
- CF nor our sub-contractors will communicate with clinicians over WhatsApp or text regarding any patient information

Standard Contractual Clauses

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR) between

NHSE (data controller)

Carnall Farrar Ltd (the data processor)

each a 'party'; together 'the parties'

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

Preamble

1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.
2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the

protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

3. In the context of the provision of support to Improving Care Coordination for Patients Programme, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.
4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.
5. Four appendices are attached to the Clauses and form an integral part of the Clauses.
6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.
7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.
8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.
9. Appendix D contains provisions for other activities which are not covered by the Clauses.
10. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.
11. The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

3. The rights and obligations of the data controller

1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State¹ data protection provisions and the Clauses.
2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

¹ References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

4. The data processor acts according to instructions

1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.
2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5. Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.
2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

6. Security of processing

1. Article 32 GDPR stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:

1. Pseudonymisation and encryption of personal data;
2. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

NOTE: THE PARTIES SHOULD FORESEE AND CONSIDER CONSEQUENCES WHICH MAY ARISE FROM ANY POTENTIALLY UNLAWFUL INSTRUCTIONS GIVEN BY THE DATA CONTROLLER AND REGULATE THIS IN AN AGREEMENT BETWEEN THE PARTIES.

c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.
3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already

implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7. Use of sub-processors

1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).
2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior authorisation of the data controller.

The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 48hrs in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

3. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection

general written authorisation

obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

5. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.
6. The data processor shall agree a third-party beneficiary clause with the sub-processor where – in the event of bankruptcy of the data processor – the data controller shall be a third-party beneficiary to the sub-processor agreement and shall have the right to enforce the agreement

against the sub-processor engaged by the data processor, e.g. enabling the data controller to instruct the sub-processor to delete or return the personal data.

7. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

8. Transfer of data to third countries or international organisations

1. Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.
2. In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.
3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:
 1. transfer personal data to a data controller or a data processor in a third country or in an international organization
 2. transfer the processing of personal data to a sub-processor in a third country
 3. have the personal data processed in by the data processor in a third country
4. The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.
5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

9. Assistance to the data controller

1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

1. the right to be informed when collecting personal data from the data subject
2. the right to be informed when personal data have not been obtained from the
data subject

3. the right of access by the data subject
4. the right to rectification
5. the right to erasure ('the right to be forgotten')
6. the right to restriction of processing
7. notification obligation regarding rectification or erasure of personal data or

restriction of processing

8. the right to data portability
9. the right to object
10. the right not to be subject to a decision based solely on automated

processing, including profiling

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:
 1. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;
 2. the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;
 3. the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);
 4. the data controller's obligation to consult the competent supervisory authority, prior to processing where a

data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

10. Notification of personal data breach

1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.
2. The data processor's notification to the data controller shall, if possible, take place within 24 hrs after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.
3. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the

data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

1. The nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
2. the likely consequences of the personal data breach;
3. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.
4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

11. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so

12. Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.
2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.
3. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

13. The parties' agreement on other terms

1. The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14. Commencement and termination

1. The Clauses shall become effective on the date of both parties' signature.
2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.
3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be

terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.
5. Signature
On behalf of the data controller

Name Position Date Signature

[NAME]

[POSITION]

[DATE]

[SIGNATURE]

Standard Contractual Clauses January 2020

On behalf of the data processor

Name Position Date Signature

15. Data controller and data processor contacts/contact points

1. The parties may contact each other using the following contacts/contact points:
2. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Name Position Telephone E-mail

Name Position Telephone E-mail

[NAME]

[POSITION]

[DATE]

[SIGNATURE]

[NAME]

[POSITION]

[TELEPHONE]

[E-MAIL]

[NAME]

[POSITION]

[TELEPHONE]

[E-MAIL]

Appendix A Information about the processing

[REDACTED]

[NOTE: IN CASE OF SEVERAL PROCESSING ACTIVITIES, THESE ELEMENTS MUST BE

[REDACTED]

COMPLETED FOR EACH OF THE PROCESSING ACTIVITIES.]

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:

[DESCRIBE THE PURPOSE OF THE PROCESSING].

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

[DESCRIBE THE NATURE OF THE PROCESSING].

A.3. The processing includes the following types of personal data about data subjects:

[DESCRIBE THE TYPE OF PERSONAL DATA BEING PROCESSED].

[FOR EXAMPLE]

"Name, e-mail address, telephone number, address, national identification number, payment details, membership number, type of membership, attendance at fitness centre and registration for specific fitness classes."

A.4. Processing includes the following categories of data subject:

[DESCRIBE CATEGORY OF DATA SUBJECT].

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

[DESCRIBE THE DURATION OF THE PROCESSING].

[NOTE: DESCRIPTION SHOULD BE MADE IN THE MOST DETAILED POSSIBLE MANNER AND, IN ANY CIRCUMSTANCE, THE TYPES OF PERSONAL DATA MUST BE SPECIFIED FURTHER THAN MERELY "PERSONAL DATA AS DEFINED IN ARTICLE 4(1) GDPR" OR STATING WHICH CATEGORY ("ARTICLE 6, 9 OG 10 GDPR") OF PERSONAL DATA IS

SUBJECT TO PROCESSING.]

Appendix B Authorised sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:

The data controller shall on the commencement of the Clauses authorise the use of the abovementioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

B.2. Prior notice for the authorisation of sub-processors

[OPTIONAL] [IF APPLICABLE, DESCRIBE THE TIME PERIODS OF PRIOR NOTICE FOR

AUTHORISATION OF SUB-PROCESSORS]

Standard Contractual Clauses January 2020

Appendix C Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

C.2. Security of processing

The level of security shall take into account:

[FOR EXAMPLE]

“That the processing involves a large volume of personal data which are subject to Article 9 GDPR on ‘special categories of personal data’ which is why a ‘high’ level of security should be established.”

The data processor shall hereafter be entitled and under obligation to make decisions about the technical and organisational security measures that are to be applied to create the necessary (and agreed) level of data security.

The data processor shall however – in any event and at a minimum – implement the following measures that have been agreed with the data controller:

[DESCRIBE THE PROCESSING THAT THE DATA PROCESSOR HAS BEEN INSTRUCTED TO PERFORM].

[TAKING INTO ACCOUNT THE NATURE, SCOPE, CONTEXT AND PURPOSES OF THE PROCESSING ACTIVITY AS WELL AS THE RISK FOR THE RIGHTS AND FREEDOMS OF NATURAL PERSONS, DESCRIBE ELEMENTS THAT ARE ESSENTIAL TO THE LEVEL OF SECURITY]

[DESCRIBE REQUIREMENTS FOR PSEUDONYMISATION AND ENCRYPTION OF PERSONAL DATA]

[DESCRIBE REQUIREMENTS FOR ENSURING ONGOING CONFIDENTIALITY, INTEGRITY, AVAILABILITY AND RESILIENCE OF PROCESSING SYSTEMS AND SERVICES]

[DESCRIBE REQUIREMENTS FOR THE ABILITY TO RESTORE THE AVAILABILITY AND ACCESS TO PERSONAL DATA IN A TIMELY MANNER IN THE EVENT OF A PHYSICAL OR TECHNICAL INCIDENT]

[DESCRIBE REQUIREMENTS FOR PROCESSES FOR REGULARLY TESTING, ASSESSING AND EVALUATING THE EFFECTIVENESS OF TECHNICAL AND ORGANISATIONAL MEASURES FOR ENSURING THE SECURITY OF THE PROCESSING]

[DESCRIBE REQUIREMENTS FOR ACCESS TO DATA ONLINE]

[DESCRIBE REQUIREMENTS FOR THE PROTECTION OF DATA DURING STORAGE]

[DESCRIBE REQUIREMENTS FOR THE PROTECTION OF DATA DURING TRANSMISSION]

[DESCRIBE REQUIREMENTS FOR PHYSICAL SECURITY OF LOCATIONS AT WHICH

PERSONAL DATA ARE PROCESSED]

[DESCRIBE REQUIREMENTS FOR THE USE OF HOME/REMOTE WORKING] [DESCRIBE REQUIREMENTS FOR LOGGING]

C.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organisational measures:

C.4. Storage period/erasure procedures

[FOR EXAMPLE]

“Personal data is stored for [STATE TIME PERIOD OR INCIDENT] after which the personal data is automatically erased by the data processor.

Upon termination of the provision of personal data processing services, the data processor shall either delete or return the personal data in accordance with Clause 11.1., unless the data controller – after the signature of the contract – has modified the data controller’s original choice. Such modification shall be documented and kept in writing, including electronically, in connection with the Clauses.”

C.5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller’s prior written authorisation:

C.6. Instruction on the transfer of personal data to third countries

[STATE THE LEGAL BASIS FOR TRANSFER PURSUANT TO CHAPTER V GDPR]

[DESCRIBE THE SCOPE AND THE EXTENT OF THE ASSISTANCE TO BE PROVIDED BY THE DATA PROCESSOR]

[DESCRIBE THE SPECIFIC TECHNICAL AND ORGANISATIONAL MEASURES TO BE TAKEN BY THE DATA PROCESSOR TO PROVIDE ASSISTANCE TO THE DATA CONTROLLER]

[STATE STORAGE PERIOD/ERASURE PROCEDURES FOR THE DATA PROCESSOR, IF APPLICABLE]

[REDACTED]

[STATE WHERE PROCESSING TAKES PLACE] [STATE THE DATA PROCESSOR OR

[REDACTED]
SUB-PROCESSOR USING THE ADDRESS]

[REDACTED]
[DESCRIBE AN INSTRUCTION ON THE TRANSFER OF PERSONAL DATA TO A THIRD

[REDACTED]
COUNTRY OR INTERNATIONAL ORGANISATION]

If the data controller does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the data processor shall not be entitled within the framework of the Clauses to perform such transfer.

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

For example:

[REDACTED]
[DESCRIBE PROCEDURES FOR THE DATA CONTROLLER'S AUDITS, INCLUDING INSPECTIONS, OF THE PROCESSING OF PERSONAL DATA BY THE DATA

[REDACTED]
PROCESSOR]

[REDACTED]
"The data processor shall [REDACTED] at
[CONTROLLER'S] expense obtain an
independent third party concerning the data processor's compliance with the GDPR, the applicable
EU or Member State data protection provisions and the Clauses.

The parties have agreed that the following types of [AUDITOR'S REPORT/INSPECTION REPORT]
may be used in compliance with the Clauses:

[INSERT 'APPROVED' AUDITOR'S REPORTS/INSPECTION REPORTS]

The **[AUDITOR'S REPORT/INSPECTION REPORT]** shall without undue delay be submitted to the data controller for information. The data controller may contest the scope and/or methodology of the report and may in such cases request a new audit/inspection under a revised scope and/or different methodology.

Based on the results of such an audit/inspection, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data controller or the data controller's representative shall in addition have access to inspect, including physically inspect, the places, where the processing of personal data is carried out by the data processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed, when the data controller deems it required."

[OR]

"The data controller or the data controller's representative shall **[STATE TIME PERIOD]** perform a physical inspection of the places, where the processing of personal data is carried out by the data processor, including physical facilities as well as systems used for and related to the processing to ascertain the data processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

In addition to the planned inspection, the data controller may perform an inspection of the data processor when the data controller deems it required"

[AND, IF APPLICABLE]

[STATE TIME PERIOD]

[THE DATA PROCESSOR'S/THE DATA

[AUDITOR'S REPORT/INSPECTION REPORT]

from an

"The data controller's costs, if applicable, relating to physical inspection shall be defrayed by the data controller. The data processor shall, however, be under obligation to set aside the resources (mainly time) required for the data controller to be able to perform the inspection."

C.8. [IF APPLICABLE] Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

[FOR EXAMPLE]

"The data processor shall at **CONTROLLER'S]** expense obtain an **[REDACTED]** from an

independent third party concerning the sub-processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The parties have agreed that the following types of [AUDITOR'S REPORT/INSPECTION REPORT] may be used in compliance with the Clauses:

[INSERT 'APPROVED' AUDITOR'S REPORTS/INSPECTION REPORTS]

The [AUDITOR'S REPORT/INSPECTION REPORT] shall without undue delay be submitted to the data controller for information. The data controller may contest the scope and/or methodology of the report and may in such cases request a new audit/inspection under a revised scope and/or different methodology.

Based on the results of such an audit/inspection, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

The data processor or the data processor's representative shall in addition have access to inspect, including physically inspect, the places, where the processing of personal data is carried out by the sub-processor, including physical facilities as well as systems used for and related to the processing. Such an inspection shall be performed, when the data processor (or the data controller) deems it required.

Documentation for such inspections shall without delay be submitted to the data controller for information. The data controller may contest the scope and/or methodology of the report and may in such cases request a new inspection under a revised scope and/or different methodology."

[OR]

"The data processor or the data processor's representative shall [STATE TIME PERIOD] perform a physical inspection of the places, where the processing of personal data is carried out by the sub-processor, including physical facilities as well as systems used for and related to the processing to ascertain the sub-processor's compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.

[IF APPLICABLE, DESCRIBE PROCEDURES FOR THE DATA CONTROLLER'S AUDITS, INCLUDING INSPECTIONS, OF PROCESSING OF PERSONAL DATA BY THE SUB-

PROCESSOR]

[STATE TIME PERIOD]

[THE DATA PROCESSOR'S/THE DATA

[AUDITOR'S REPORT/INSPECTION REPORT]

In addition to the planned inspection, the data processor may perform an inspection of the sub-processor when the data processor (or the data controller) deems it required.

Documentation for such inspections shall without undue delay be submitted to the data controller for information. The data controller may contest the scope and/or methodology of the report and may in such cases request a new inspection under a revised scope and/or different methodology.

Based on the results of such an inspection, the data controller may request further measures to be taken to ensure compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.”

[AND, IF APPLICABLE]

“The data controller may – if required – elect to initiate and participate in a physical inspection of the sub-processor. This may apply if the data controller deems that the data processor’s supervision of the sub-processor has not provided the data controller with sufficient documentation to determine that the processing by the sub-processor is being performed according to the Clauses.

The data controller’s participation in an inspection of the sub-processor shall not alter the fact that the data processor hereafter continues to bear the full responsibility for the sub-processor’s compliance with the GDPR, the applicable EU or Member State data protection provisions and the Clauses.”

[AND, IF APPLICABLE]

“The data processor’s and the sub-processor’s costs related to physical supervision/inspection at the sub-processor’s facilities shall not concern the data controller – irrespective of whether the data controller has initiated and participated in such inspection.”

Annex 8

Acceptance Testing

Not Used.