

Joint Schedule 11 (Processing Data)

Status of the Controller

1. The Parties acknowledge that for the purposes of the Data Protection Legislation, the nature of the activity carried out by each of them in relation to their respective obligations under a Contract dictates the status of each party under the DPA. A Party may act as:
 - (a) "Controller" in respect of the other Party who is "Processor";
 - (b) "Processor" in respect of the other Party who is "Controller";
 - (c) "Sub-Processor" in respect of the other Party who is "Processor";
 - (d) "Joint Controller" with the other Party;
 - (e) "Independent Controller" of the Personal Data where there other Party is also "Controller",

in respect of certain Personal Data under a Contract and shall specify in Annex 1 (*Processing Personal Data*) which scenario they think shall apply in each situation.

Where one Party is Controller and the other Party its Processor

2. Where a Party is a Processor, the only Processing that it is authorised to do is listed in Annex 1 (*Processing Personal Data*) by the Controller.
3. The Processor shall notify the Controller immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.
4. The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:
 - (a) a systematic description of the envisaged Processing and the purpose of the Processing;
 - (b) an assessment of the necessity and proportionality of the Processing in relation to the Services;
 - (c) an assessment of the risks to the rights and freedoms of Data Subjects; and
 - (d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
5. The Processor shall, in relation to any Personal Data Processed in connection with its obligations under the Contract:

Joint Schedule 11 (Processing Data)

Crown Copyright 2018

- (a) Process that Personal Data only in accordance with Annex 1 (*Processing Personal Data*) unless the Processor is required to do otherwise by Law. If it is so required the Processor shall notify the Controller before Processing the Personal Data unless prohibited by Law;
- (b) ensure that it has in place Protective Measures, including in the case of the Supplier the measures set out in Clause 14.3 of the Core Terms, which the Controller may reasonably reject (but failure to reject shall not amount to approval by the Controller of the adequacy of the Protective Measures) having taken account of the:
 - (i) nature of the data to be protected;
 - (ii) harm that might result from a Personal Data Breach;
 - (iii) state of technological development; and
 - (iv) cost of implementing any measures;
- (c) ensure that :
 - (i) the Processor Personnel do not Process Personal Data except in accordance with the Contract (and in particular Annex 1 (*Processing Personal Data*));
 - (ii) it takes all reasonable steps to ensure the reliability and integrity of any Processor Personnel who have access to the Personal Data and ensure that they:
 - (A) are aware of and comply with the Processor's duties under this Joint Schedule 11, Clauses 14 (*Data protection*), 15 (*What you must keep confidential*) and 16 (*When you can share information*);
 - (B) are subject to appropriate confidentiality undertakings with the Processor or any Sub-Processor;
 - (C) are informed of the confidential nature of the Personal Data and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by the Contract; and
 - (D) have undergone adequate training in the use, care, protection and handling of Personal Data;
- (d) not transfer Personal Data outside of the EU unless the prior written consent of the Controller has been obtained and the following conditions are fulfilled:
 - (i) the Controller or the Processor has provided appropriate safeguards in relation to the transfer (whether in accordance with GDPR Article 46 or LED Article 37) as determined by the Controller;
 - (ii) the Data Subject has enforceable rights and effective legal remedies;
 - (iii) the Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection

- to any Personal Data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Controller in meeting its obligations); and
- (iv) the Processor complies with any reasonable instructions notified to it in advance by the Controller with respect to the Processing of the Personal Data; and
 - (e) at the written direction of the Controller, delete or return Personal Data (and any copies of it) to the Controller on termination of the Contract unless the Processor is required by Law to retain the Personal Data.
6. Subject to paragraph 7 of this Joint Schedule 11, the Processor shall notify the Controller immediately if in relation to it Processing Personal Data under or in connection with the Contract it:
- (a) receives a Data Subject Access Request (or purported Data Subject Access Request);
 - (b) receives a request to rectify, block or erase any Personal Data;
 - (c) receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;
 - (d) receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under the Contract;
 - (e) receives a request from any third Party for disclosure of Personal Data where compliance with such request is required or purported to be required by Law; or
 - (f) becomes aware of a Personal Data Breach.
7. The Processor's obligation to notify under paragraph 6 of this Joint Schedule 11 shall include the provision of further information to the Controller, as details become available.
8. Taking into account the nature of the Processing, the Processor shall provide the Controller with assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 6 of this Joint Schedule 11 (and insofar as possible within the timescales reasonably required by the Controller) including by immediately providing:
- (a) the Controller with full details and copies of the complaint, communication or request;
 - (b) such assistance as is reasonably requested by the Controller to enable it to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
 - (c) the Controller, at its request, with any Personal Data it holds in relation to a Data Subject;
 - (d) assistance as requested by the Controller following any Personal Data Breach; and/or

Joint Schedule 11 (Processing Data)

Crown Copyright 2018

- (e) assistance as requested by the Controller with respect to any request from the Information Commissioner's Office, or any consultation by the Controller with the Information Commissioner's Office.
- 9. The Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Joint Schedule 11. This requirement does not apply where the Processor employs fewer than 250 staff, unless:
 - (a) the Controller determines that the Processing is not occasional;
 - (b) the Controller determines the Processing includes special categories of data as referred to in Article 9(1) of the GDPR or Personal Data relating to criminal convictions and offences referred to in Article 10 of the GDPR; or
 - (c) the Controller determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.
- 10. The Processor shall allow for audits of its Data Processing activity by the Controller or the Controller's designated auditor.
- 11. The Parties shall designate a Data Protection Officer if required by the Data Protection Legislation.
- 12. Before allowing any Sub-Processor to Process any Personal Data related to the Contract, the Processor must:
 - (a) notify the Controller in writing of the intended Sub-Processor and Processing;
 - (b) obtain the written consent of the Controller;
 - (c) enter into a written agreement with the Sub-Processor which give effect to the terms set out in this Joint Schedule 11 such that they apply to the Sub-Processor; and
 - (d) provide the Controller with such information regarding the Sub-Processor as the Controller may reasonably require.
- 13. The Processor shall remain fully liable for all acts or omissions of any of its Sub-Processors.
- 14. The Relevant Authority may, at any time on not less than 30 Working Days' notice, revise this Joint Schedule 11 by replacing it with any applicable Controller to Processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to the Contract).
- 15. The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Relevant Authority may on not less than 30 Working Days' notice to the Supplier amend the Contract to ensure that it complies with any guidance issued by the Information Commissioner's Office.

Where the Parties are Joint Controllers of Personal Data


16. In the event that the Parties are Joint Controllers in respect of Personal Data under the Contract, the Parties shall implement paragraphs that are necessary to comply with GDPR Article 26 based on the terms set out in Annex 2 to this Joint Schedule 11 (*Processing Data*).

Independent Controllers of Personal Data

17. With respect to Personal Data provided by one Party to another Party for which each Party acts as Controller but which is not under the Joint Control of the Parties, each Party undertakes to comply with the applicable Data Protection Legislation in respect of their Processing of such Personal Data as Controller.
18. Each Party shall Process the Personal Data in compliance with its obligations under the Data Protection Legislation and not do anything to cause the other Party to be in breach of it.
19. Where a Party has provided Personal Data to the other Party in accordance with paragraph 7 of this Joint Schedule 11 above, the recipient of the Personal Data will provide all such relevant documents and information relating to its data protection policies and procedures as the other Party may reasonably require.
20. The Parties shall be responsible for their own compliance with Articles 13 and 14 GDPR in respect of the Processing of Personal Data for the purposes of the Contract.
21. The Parties shall only provide Personal Data to each other:
- (a) to the extent necessary to perform their respective obligations under the Contract;
 - (b) in compliance with the Data Protection Legislation (including by ensuring all required data privacy information has been given to affected Data Subjects to meet the requirements of Articles 13 and 14 of the GDPR); and
 - (c) where it has recorded it in Annex 1 (*Processing Personal Data*).
22. 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, each Party shall, with respect to its Processing of Personal Data as Independent Controller, implement and maintain appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1)(a), (b), (c) and (d) of the GDPR, and the measures shall, at a minimum, comply with the requirements of the Data Protection Legislation, including Article 32 of the GDPR.
23. A Party Processing Personal Data for the purposes of the Contract shall maintain a record of its Processing activities in accordance with Article 30

GDPR and shall make the record available to the other Party upon reasonable request.

24. Where a Party receives a request by any Data Subject to exercise any of their rights under the Data Protection Legislation in relation to the Personal Data provided to it by the other Party pursuant to the Contract (**“Request Recipient”**):
- (a) the other Party shall provide any information and/or assistance as reasonably requested by the Request Recipient to help it respond to the request or correspondence, at the cost of the Request Recipient; or
 - (b) where the request or correspondence is directed to the other Party and/or relates to that other Party's Processing of the Personal Data, the Request Recipient will:
 - (i) promptly, and in any event within five (5) Working Days of receipt of the request or correspondence, inform the other Party that it has received the same and shall forward such request or correspondence to the other Party; and
 - (ii) provide any information and/or assistance as reasonably requested by the other Party to help it respond to the request or correspondence in the timeframes specified by Data Protection Legislation.
25. Each Party shall promptly notify the other Party upon it becoming aware of any Personal Data Breach relating to Personal Data provided by the other Party pursuant to the Contract and shall:
- (a) do all such things as reasonably necessary to assist the other Party in mitigating the effects of the Personal Data Breach;
 - (b) implement any measures necessary to restore the security of any compromised Personal Data;
 - (c) work with the other Party to make any required notifications to the Information Commissioner's Office and affected Data Subjects in accordance with the Data Protection Legislation (including the timeframes set out therein); and
 - (d) not do anything which may damage the reputation of the other Party or that Party's relationship with the relevant Data Subjects, save as required by Law.
26. Personal Data provided by one Party to the other Party may be used exclusively to exercise rights and obligations under the Contract as specified in Annex 1 (*Processing Personal Data*).
27. Personal Data shall not be retained or processed for longer than is necessary to perform each Party's respective obligations under the Contract which is specified in Annex 1 (*Processing Personal Data*).



Joint Schedule 11 (Processing Data)

Crown Copyright 2018

28. Notwithstanding the general application of paragraphs 2 to 15 of this Joint Schedule 11 to Personal Data, where the Supplier is required to exercise its regulatory and/or legal obligations in respect of Personal Data, it shall act as an Independent Controller of Personal Data in accordance with paragraphs 16 to 27 of this Joint Schedule 11.

Annex 1 - Processing Personal Data

- 1.1 The contact details of the Relevant Authority's Data Protection Officer are: [REDACTED]
- 1.2 The contact details of the Supplier's Data Protection Officer are: [REDACTED]
- 1.3 The Processor shall comply with any further written instructions with respect to Processing by the Controller.
- 1.4 Any such further instructions shall be incorporated into this Annex.

Description	Details
Identity of Controller for each Category of Personal Data	<p>The customer of the Relevant Authority is Controller, the Relevant Authority is the Processor and the Supplier is Sub-Processor.</p> <p>The Parties acknowledge that in accordance with paragraph 2 to paragraph 15 and for the purposes of the Data Protection Legislation, the customer of the Relevant Authority is Controller, the Relevant Authority is the Processor, and the Supplier is Sub-Process:</p> <ul style="list-style-type: none">• Business contact details of Supplier Personnel for which the Supplier is the Sub-Processor,• Business contact details of any directors, officers, employees, agents, consultants and contractors of CCS (excluding the Supplier Personnel) engaged in the performance of the CCS' duties under the Contract for which CCS is the Controller. <p>All organisations considering applying to NHS Digital for access to identifiable (or pseudonymised) data must first enter into an overarching Data Sharing Framework Contract (DSFC) with NHS Digital. This forms the basis for the ongoing relationship with NHS Digital as it outlines expectations for governance, security standards, retention and destruction of data as well as NHS Digital audit rights.</p> <p>Upon Research Ethics Committee (REC) approval, and Confidentiality Advisory Group (CAG) for Section 251 support for the NHS DigiTrials Recruitment Service, the Data Sharing Agreement (DSA) is processed. A formal opinion is then sought and obtained from Independent Group Advising on the Release of Data (IGARD).</p> <p>The DSA governs what and how the data that is the subject of the DARs application can be processed.</p>

Joint Schedule 11 (Processing Data)

Crown Copyright 2018

	<p>NHS Digital is data Processor for the purposes of sending invites and communications. NHS Digital transfers the data to the mailing provider, who is the Sub-Processor, to conduct the mailout (on behalf of the customer).</p> <p>The Sub-Processor is responsible for carrying out the processing of patient data in line with the data processing agreement/ contract that it has with NHS Digital i.e. to send the approved invitation letters and communications to the listed cohort.</p>
Duration of the Processing	<p>The Framework Contract Period and thereafter, until expiry or termination of the last Call-Off Contract under the Framework, including the period until all transactions relating to Call-Off Contracts have permanently ceased.</p> <p>Processing will take place throughout the duration of the contract, at the request of NHS Digital. When the supplier is notified, the submitted cohort will be processed.</p>
Nature and purposes of the Processing	<p>For both the Recruitment and Communications Service, under a Data Sharing Agreement and Data Processing Agreement, a file containing details of those to be contacted is sent to NHS Digital's securely contracted mailing provider via Secure Electronic File Transfer (SEFT).</p> <p>No new data collection is planned in order to provide the NHS DigiTrials Recruitment service, however temporary data assets are created as a result of the Directed analysis and linkage.</p> <p>The Sub-Processor (mailing provider) shall retain each cohort for 10 working days after the invitation or communication has been issued, but delete the cohort data within 20 working days after the invitation or communication has been issued.</p>
Type of Personal Data	<p>The following information will be provided to the mailing provider in order for them to disseminate the invitations. A template of the output containing such information will be provided under version control.</p> <ol style="list-style-type: none">1. Title2. Family Name3. Given Name4. Address line 15. Address line 26. Address line 37. Address link 4

Joint Schedule 11 (Processing Data)

Crown Copyright 2018

	<p>8. Postcode</p> <p>9. Email address</p> <p>10. Contact number</p> <p>11. Accessibility information (e.g. large print)</p> <p>12. Language preferences</p> <p>Personal details of each Party's Personnel engaged in the performance of obligations and day to day management of the Framework Contract:</p> <ul style="list-style-type: none">• Full name• Job title• Organisation name• Business/workplace address• Business/workplace email address• Business/workplace telephone/mobile number(s)• Supplier Personnel date of birth (when required for security purposes when Supplier Personnel visit CCS premises)• Supplier [REDACTED] System ([REDACTED])• Registered company details including registered company name, address and company registration number (CRN)• Bank account details for activities related to the Management Charge• Management Information
Categories of Data Subject	<p>Personnel data of the Parties involved in the performance of obligations and day to day management of the Framework Contract.</p> <p>NHS DigiTrials Recruitment service – data subjects are identified through analysis and linkage of national datasets to identify they as potentially eligible for a particular clinical trial</p> <p>NHS DigiTrials Communications service – data subjects are individuals that have consented through clear consent materials to take part in a clinical trial, including the dissemination of their information to NHS Digital and its Sub Processors.</p>