

**Template Sub-Contract for use with NHS Standard Contract 2017/18 and 2018/19**

**(Shorter Form)**

**Schedule 6F Sub-Contractor Data Processing Agreement**

**July 2018**

**Template Sub-Contract for use with NHS Standard Contract 2017/18 and 2018/19 (Shorter Form)**

**Schedule 6F Sub-Contractor Data Processing Agreement**

**July 2018 edition**

First published: July 2018

Prepared by: NHS Standard Contract Team

nhscb.contractshelp@nhs.net

Publications Gateway Reference: 08283

Document Classification: Official

**SCHEDULE 6 – CONTRACT MANAGEMENT, REPORTING AND INFORMATION REQUIREMENTS**

**F. Sub-Contractor Data Processing Agreement**

*NOTE: This Schedule 6F applies only where the Sub-Contractor is appointed to act as a Data Processor or Sub-processor under this Sub-Contract. Where the Head Provider is acting as Data Controller in respect of the relevant data, it may appoint the Sub-Contractor to act as a Data Processor in relation to that data; where the Head Provider is itself appointed to act as a Data Processor by one or more Commissioners under the Head Contract, it may appoint the Sub-Contractor to act as a Sub-processor under this Sub-Contract. Delete/populate this Schedule if and as applicable.*

1. **SCOPE**
   1. The Head Provider appoints the Sub-Contractor as a [Data Processor/Sub-processor] to perform the Data Processing Services.
   2. When delivering the Data Processing Services, the Sub-Contractor must, in addition to its other obligations under this Contract, comply with the provisions of this Schedule 6F.
   3. This Schedule 6F applies for so long as the Sub-Contractor acts as a [Data Processor/Sub-processor] in connection with this Contract.
2. **DATA PROTECTION**
   1. The Parties acknowledge that for the purposes of Data Protection Legislation in relation to the Data Processing Services [the Head Provider is the Data Controller and the Sub-Contractor is the Data Processor] [the [Co-ordinating] Commissioner is the Data Controller, the Head Provider is the Data Processor and the Sub-Contractor is the Sub-processor]. The Sub-Contractor must process the Processor Data only to the extent necessary to perform the Data Processing Services and only in accordance with written instructions set out in this Schedule, including instructions regarding transfers of Personal Data outside the EU or to an international organisation unless such transfer is required by Law, in which case the Sub-Contractor must inform the Head Provider [and the Co-ordinating Commissioner] of that requirement before processing takes place, unless this is prohibited by Law on the grounds of public interest.
   2. The Sub-Contractor must notify the Head Provider [and the Co-ordinating Commissioner] immediately if it considers that carrying out any of the Head Provider’s instructions would infringe Data Protection Legislation.
   3. The Sub-Contractor must provide all reasonable assistance to the Head Provider [and/or the Co-ordinating Commissioner] in the preparation of any Data Protection Impact Assessment prior to commencing any processing. Such assistance may, at the discretion of the Head Provider [and/or the Co-ordinating Commissioner] , include:
      1. a systematic description of the envisaged processing operations and the purpose of the processing;
      2. an assessment of the necessity and proportionality of the processing operations in relation to the Data Processing Services;
      3. an assessment of the risks to the rights and freedoms of Data Subjects; and
      4. the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data.
   4. The Sub-Contractor must, in relation to any Personal Data processed in connection with its obligations under this Schedule 6F:
      1. process that Personal Data only in accordance with Annex A, unless the Sub-Contractor is required to do otherwise by Law. If it is so required the Sub-Contractor must promptly notify the Head Provider [and the Co-ordinating Commissioner] before processing the Personal Data unless prohibited by Law;
      2. ensure that it has in place Protective Measures, which have been reviewed and approved by the Head Provider as appropriate to protect against a Data Loss Event having taken account of the:
         1. nature of the data to be protected;
         2. harm that might result from a Data Loss Event;
         3. state of technological development; and
         4. cost of implementing any measures;
      3. ensure that:
         1. when delivering the Data Processing Services the Sub-Contractor’s Staff only process Personal Data in accordance with this Schedule 6F (and in particular Annex A);
         2. it takes all reasonable steps to ensure the reliability and integrity of any Sub-Contractor’s Staff who have access to the Personal Data and ensure that they:
            1. are aware of and comply with the Sub-Contractor’s duties under this paragraph;
            2. are subject to appropriate confidentiality undertakings with the Sub-Contractor and any [further] Sub-processor;
            3. 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 Head Provider or as otherwise permitted by this Sub-Contract;
            4. have undergone adequate training in the use, care, protection and handling of Personal Data; and
            5. are aware of and trained in the policies and procedures identified in GC21.11 (*Patient Confidentiality, Data Protection, Freedom of Information and Transparency*) of the NHS Standard Contract.
      4. not transfer Personal Data outside of the EU unless the prior written consent of the Head Provider [and the Co-ordinating Commissioner] has been obtained and the following conditions are fulfilled:
         1. the Head Provider or the Sub-Contractor has provided appropriate safeguards in relation to the transfer as determined by the Head Provider [and the Co-ordinating Commissioner];
         2. the Data Subject has enforceable rights and effective legal remedies;
         3. the Sub-Contractor complies with its obligations under 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 Head Provider and the Commissioners in meeting their obligations); and
         4. the Sub-Contractor complies with any reasonable instructions notified to it in advance by the Head Provider with respect to the processing of the Personal Data;
      5. at the written direction of the Head Provider, delete or return Personal Data (and any copies of it) to the Head Provider [or the Co-ordinating Commissioner, as appropriate] on termination of the Data Processing Services and certify to the Head Provider [and the Co-ordinating Commissioner] that it has done so within five Operational Days of any such instructions being issued, unless the Sub-Contractor is required by Law to retain the Personal Data;
      6. if the Sub-Contractor is required by any Law or Regulatory or Supervisory Body to retain any Processor Data that it would otherwise be required to destroy under this paragraph 2.4, notify the Head Provider [and the Co-ordinating Commissioner] in writing of that retention giving details of the Processor Data that it must retain and the reasons for its retention; and
      7. co-operate fully with the Head Provider [and the Co-ordinating Commissioner] during any handover arising from the cessation of any part of the Data Processing Services, and if the Head Provider directs the Sub-Contractor to migrate Processor Data to the Head Provider, or to a Commissioner or to a third party, provide all reasonable assistance with ensuring safe migration including ensuring the integrity of Processor Data and the nomination of a named point of contact for the Head Provider [and the Co-ordinating Commissioner].
   5. Subject to paragraph 2.6, the Sub-Contractor must notify the Head Provider [and the Co-ordinating Commissioner] immediately if, in relation any Personal Data processed in connection with its obligations under this Schedule 6F, it:
      1. receives a Data Subject Access Request (or purported Data Subject Access Request);
      2. receives a request to rectify, block or erase any Personal Data;
      3. receives any other request, complaint or communication relating to obligations under Data Protection Legislation owed by the Sub-Contractor, the Head Provider or any Commissioner;
      4. receives any communication from the Information Commissioner or any other Regulatory or Supervisory Body (including any communication concerned with the systems on which Personal Data is processed under this Schedule 6F);
      5. 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;
      6. becomes aware of or reasonably suspects a Data Loss Event; or
      7. becomes aware of or reasonably suspects that it has in any way caused the Head Provider or any Commissioner to breach Data Protection Legislation.
   6. The Sub-Contractor’s obligation to notify under paragraph 2.5 includes the provision of further information to the Head Provider [and the Co-ordinating Commissioner] in phases, as details become available.
   7. The Sub-Contractor must provide whatever co-operation the Head Provider [and/or the Co-ordinating Commissioner] reasonably requires to remedy any issue notified to the Head Provider [and the Co-ordinating Commissioner] under paragraphs 2.5 and 2.6 as soon as reasonably practicable.
   8. Taking into account the nature of the processing, the Sub-Contractor must provide the Head Provider [and/or the Co-ordinating Commissioner] with full assistance in relation to either Party's (or any Commissioner’s) obligations under Data Protection Legislation and any complaint, communication or request made under paragraph 2.5 (and insofar as possible within the timescales reasonably required by the Head Provider [and/or the Co-ordinating Commissioner]) including by promptly providing:
      1. the Head Provider [and the Co-ordinating Commissioner] with full details and copies of the complaint, communication or request;
      2. such assistance as is reasonably requested by the Head Provider [and/or the Co-ordinating Commissioner] to enable the Head Provider and/or the Co-ordinating Commissioner to comply with a Data Subject Access Request within the relevant timescales set out in Data Protection Legislation;
      3. assistance as requested by the Head Provider [and/or the Co-ordinating Commissioner] following any Data Loss Event;
      4. assistance as requested by the Head Provider [and/or the Co-ordinating Commissioner] with respect to any request from the Information Commissioner’s Office, or any consultation by the Head Provider or the Co-ordinating Commissioner with the Information Commissioner's Office.
   9. Without prejudice to the generality of GC15 *(Governance, Transaction Records and Audit)* of the NHS Standard Contract,the Sub-Contractor must allow for audits of its delivery of the Data Processing Services by the Head Provider, the Co-ordinating Commissioner or either’s designated auditor.
   10. For the avoidance of doubt the provisions of GC12 *(Assignment and Sub-contracting)* of the NHS Standard Contract and Sub-Contract General Conditions 3.20 – 3.22 apply to the delivery of any Data Processing Services.
   11. Without prejudice to GC12, before allowing any Sub-processor to process any Personal Data related to this Schedule 6F, the Sub-Contractor must:
       1. notify the Head Provider [(and if the Head Provider is a Data Processor regarding the Data Processing Services the relevant Data Controller)] in writing of the intended Sub-processor and processing;
       2. obtain the written consent of the Head Provider [(and if the Head Provider is a Data Processor regarding the Data Processing Services the relevant Data Controller)];
       3. carry out appropriate due diligence of the Sub-processor and ensure this is documented;
       4. enter into a binding written agreement with the Sub-processor which as far as practicable includes equivalent terms to those set out in this Schedule 6F and in any event includes the requirements set out at GC 21.15.2 of the NHS Standard Contract; and
       5. provide the Head Provider [(and if the Head Provider is a Data Processor regarding the Data Processing Services the relevant Data Controller)] with such information regarding the Sub-processor as the Head Provider [(and if the Head Provider is also a Data Processor regarding the Data Processing Services the relevant Data Controller)] may reasonably require.
   12. The Sub-Contractor must create and maintain a record of all categories of data processing activities carried out under this Schedule 6F, containing:
       1. the categories of processing carried out under this Schedule 6F;
       2. where applicable, transfers of Personal Data to a third country or an international organisation, including the identification of that third country or international organisation and, where relevant, the documentation of suitable safeguards;
       3. a general description of the Protective Measures taken to ensure the security and integrity of the Personal Data processed under this Schedule 6F; and
       4. a log recording the processing of the Processor Data by or on behalf of the Sub-Contractor comprising, as a minimum, details of the Processor Data concerned, how the Processor Data was processed, when the Processor Data was processed and the identity of any individual carrying out the processing.
   13. The Sub-Contractor warrants and undertakes that it will deliver the Data Processing Services in accordance with all Data Protection Legislation and this Sub-Contract and in particular that it has in place Protective Measures that are sufficient to ensure that the delivery of the Data Processing Services complies with Data Protection Legislation and ensures that the rights of Data Subjects are protected.
   14. The Sub-Contractor must comply at all times with obligations equivalent to those imposed on the Head Provider [(and/or if the Head Provider is a Data Processor regarding the Data Processing Services those obligations imposed on the relevant Data Controller)] by virtue of Seventh Data Protection Principle for so long as the DPA 1998 remains in force and after that time with those set out at Article 32 of the GDPR and equivalent provisions implemented into Law.
   15. The Sub-Contractor must assist the Head Provider and the Commissioners in ensuring compliance with the obligations set out at Article 32 to 36 of the GDPR and equivalent provisions implemented into Law, taking into account the nature of processing and the information available to the Sub-Contractor.
   16. The Sub-Contractor must take prompt and proper remedial action regarding any Data Loss Event.
   17. The Sub-Contractor must assist the Head Provider and the Commissioners by taking appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Head Provider’s and the Commissioners’ obligations to respond to requests for exercising rights granted to individuals by Data Protection Legislation.

**Annex A**

**Data Processing Services**

**Processing, Personal Data and Data Subjects**

1. The Sub-Contractor must comply with any further written instructions with respect to [sub-]processing by the Head Provider.
2. Any such further instructions shall be incorporated into this Annex.

| **Description** | **Details** |
| --- | --- |
| Subject matter of the [sub-]processing | *[This should be a high level, short description of what the processing is about i.e. its subject matter]* |
| Duration of the [sub-]processing | *[Clearly set out the duration of the processing including dates]* |
| Nature and purposes of the [sub-]processing | *[Please be as specific as possible, but make sure that you cover all intended purposes. The nature of the processing means any operation such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction of data (whether or not by automated means) etc. The purpose might include: employment processing, statutory obligation, recruitment assessment etc]* |
| Type of Personal Data | *[Examples here include: name, address, date of birth, NI number, telephone number, pay, images, biometric data etc]* |
| Categories of Data Subject | *[Examples include: Staff (including volunteers, agents, and temporary workers), Commissioners/ clients, suppliers, patients, students / pupils, members of the public, users of a particular website etc]* |
| Plan for return and destruction of the data once the [sub-]processing is complete UNLESS requirement under union or member state law to preserve that type of data | *[Describe how long the data will be retained for, how it be returned or destroyed]* |

**Annex B - Definitions**

In this Schedule 6F the following words and phrases have the following meanings:

**Data Processing Services** the data processing services described in Annex A to this Schedule 6F

**Data Protection Impact Assessment** an assessment by the Controller of the impact of the envisaged processing on the protection of Personal Data

**Data Loss Event** any event that results, or may result, in unauthorised processing of Personal Data held by the Sub-Contractor under this Sub-Contract or Personal Data for which the Sub-Contractor has responsibility under this Sub-Contract including without limitation actual or potential loss, destruction, corruption or inaccessibility of Personal Data, including any Personal Data Breach

**Data Subject Access Request** a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to Data Protection Legislation to access their Personal Data

**Processor Data** is any data processed by the Sub-Contractor in connection with the Data Processing Services

**Protective Measures** appropriate technical and organisational measures which may include: pseudonymising 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

© Crown copyright 2018

First published: July 2018

Published in electronic format only