NHS England

NHS Standard Contract 2017/18 and 2018/19 Particulars (Shorter Form)

Schedule 6F
March 2018 *Draft for consultation*

NHS Standard Contract 2017/18 and 2018/19

Particulars (Shorter Form)

Schedule 6F

March 2018 edition *Draft for consultation*

First published: March 2018 (draft)

Prepared by: NHS Standard Contract Team

nhscb.contractshelp@nhs.net

Publications Gateway Reference: 07759

Document Classification: Official

SCHEDULE 6 – CONTRACT MANAGEMENT, REPORTING AND INFORMATION REQUIREMENTS

F. Provider Data Processing Agreement

***[Drafting note**: Where practical we have adopted the standard wording given in the Procurement Policy Note (PPN) 03/17: Changes to Data Protection Legislation & General Data Protection Regulation (https://www.gov.uk/government/publications/procurement-policy-note-0317). We have departed from that wording in places to ensure consistency with other parts of the contract or where we considered additional clarification was required.*

Many of the clauses set out here must be included in the contract in order to comply with article 28. We have taken the view that it is not practical to say that only some of the clauses need to be incorporated into existing contracts. Therefore, under our proposals this contract would need to be incorporated in its entirety into existing contracts where the Provider is acting as a data processor.]

1. SCOPE

1.1 The Co-ordinating Commissioner appoints the Provider as a Data Processor to perform the Data Processing Services.

1.2 When delivering the Data Processing Services, the Provider must, in addition to its other obligations under this Contract, comply with the provisions of this Schedule 6F.

1.3 This Schedule 6F applies for so long as the Provider acts as a Data Processor in connection with this Contract.

2. DATA PROTECTION

2.1 The Parties acknowledge that for the purposes of Data Protection Legislation in relation to the Data Processing Services the Co-ordinating Commissioner is the Data Controller and the Provider is the Data Processor. The Provider 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 Data Processor shall inform the Provider of that requirement before processing takes place, unless this is prohibited by Law on the grounds of public interest.

2.2 The Provider must notify the Co-ordinating Commissioner immediately if it considers that carrying out any of the Co-ordinating Commissioner's instructions would infringe Data Protection Legislation.

2.3 The Provider must provide all reasonable assistance to 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 Co-ordinating Commissioner, include:

(a) a systematic description of the envisaged processing operations and the purpose of the processing;

(b) an assessment of the necessity and proportionality of the processing operations in relation to the Data Processing 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.

2.4 The Provider must, in relation to any Personal Data processed in connection with its obligations under this Schedule 6F:

(a) process that Personal Data only in accordance with Annex A, unless the Provider is required to do otherwise by Law. If it is so required the Provider must promptly notify the Co-ordinating Commissioner before processing the Personal Data unless prohibited by Law;

(b) ensure that it has in place Protective Measures, which have been reviewed and approved by the Co-ordinating Commissioner as appropriate to protect against a Data Loss Event having taken account of the:

(i) nature of the data to be protected;

(ii) harm that might result from a Data Loss Event;

(iii) state of technological development; and

(iv) cost of implementing any measures;

(c) ensure that:

(i) when delivering the Data Processing Services the Provider Staff only process Personal Data in accordance with this Schedule 6F (and in particular Annex A);

(ii) it takes all reasonable steps to ensure the reliability and integrity of any Provider Staff who have access to the Personal Data and ensure that they:

(A) are aware of and comply with the Provider's duties under this clause;

(B) are subject to appropriate confidentiality undertakings with the Provider and 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 Co-ordinating Commissioner or as otherwise permitted by this Contract;

(D) have undergone adequate training in the use, care, protection and handling of Personal Data; and

(E) are aware of and trained in the policies and procedures identified in GC21.11 (*Patient Confidentiality, Data Protection, Freedom of Information and Transparency*).

(d) not transfer Personal Data outside of the EU unless the prior written consent of the Co-ordinating Commissioner has been obtained and the following conditions are fulfilled:

(i) the Co-ordinating Commissioner or the Provider has provided appropriate safeguards in relation to the transfer as determined by the Co-ordinating Commissioner;

(ii) the Data Subject has enforceable rights and effective legal remedies;

(iii) the Provider 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 Co-ordinating Commissioner in meeting its obligations); and

(iv) the Provider complies with any reasonable instructions notified to it in advance by the Co-ordinating Commissioner with respect to the processing of the Personal Data; and

(e) at the written direction of the Co-ordinating Commissioner, delete or return Personal Data (and any copies of it) to the Co-ordinating Commissioner on termination of the Data Processing Services and certify to the Co-ordinating Commissioner that it has done so within five Operational Days of any such instructions being issued, unless the Provider is required by Law to retain the Personal Data.

(f) if the Provider 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 Co-ordinating Commissioner in writing of that retention giving details of the Processor Data that it must retain and the reasons for its retention.

(g) co-operate fully with the Co-ordinating Commissioner during any handover arising from the cessation of any part of the Data Processing Services, and if the Co-ordinating Commissioner directs the Provider to migrate Processor Data to the Co-ordinating 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 Co-ordinating Commissioner.

2.5 Subject to paragraph 2.6, the Provider must notify the Co-ordinating Commissioner immediately if 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 obligations under Data Protection Legislation owed by the Provider or any Commissioner;

(d) receives any communication from the Information Commissioner or any other Regulatory or Supervisory Body in connection with Personal Data processed under this Schedule 6F including any communication concerned with the systems on which Personal Data is processed under this Schedule 6F;

(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;

(f) becomes aware of or reasonably suspects a Data Loss Event; or

(g) becomes aware of or reasonably suspects that it has in any way caused the Co-ordinating Commissioner or other Commissioner to breach Data Protection Legislation.

2.6 The Provider's obligation to notify under paragraph 2.5 includes the provision of further information to the Co-ordinating Commissioner in phases, as details become available.

2.7 The Provider must provide whatever co-operation the Co-ordinating Commissioner reasonably requires to remedy any issue notified to the Co-ordinating Commissioner under paragraphs 2.5 and 2.6 as soon as reasonably practicable.

2.8 Taking into account the nature of the processing, the Provider must provide the Co-ordinating Commissioner with full assistance in relation to either Party'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 Co-ordinating Commissioner) including by promptly providing:

(a) the Co-ordinating Commissioner with full details and copies of the complaint, communication or request;

(b) such assistance as is reasonably requested by the Co-ordinating Commissioner to enable the Co-ordinating Commissioner to comply with a Data Subject Access Request within the relevant timescales set out in Data Protection Legislation;

***[Drafting Note**: We have not included point (c) from the PPN drafting, which requires the processor (Provider) to provide personal data to the controller (Co-ordinating Commissioner) on request. This is because there is a risk that this may not comply with the law of confidentiality.]*

(c) assistance as requested by the Co-ordinating Commissioner following any Data Loss Event;

(d) assistance as requested by the Co-ordinating Commissioner with respect to any request from the Information Commissioner's Office, or any consultation by the Co-ordinating Commissioner with the Information Commissioner's Office.

2.9 Without prejudice to the generality of GC15 *(Governance, Transaction Records and Audit),* the Provider must allow for audits of its delivery of the Data Processing Services by the Co-ordinating Commissioner or the Co-ordinating Commissioner's designated auditor.

***[Drafting Note**: We have not included the provision in the PPN about maintaining a record of processing as we have dealt with this in a new clause below. That clause requires the provider to maintain this record. This is because in the vast majority, if not all, cases the Provider will be processing health data.]*

***[Drafting Note**: We have not included the provision in the PPN that states that the processor (Provider) must appoint a DPO if required by Data Protection Legislation. This is because we have included a provision in the GCs that requires the Provider to appoint a DPO in any case.]*

2.10 For the avoidance of doubt the provisions of GC12 *(Assignment and Sub-contracting)* apply to the delivery of any Data Processing Services.

2.11 Without prejudice to GC12, before allowing any Sub-processor to process any Personal Data related to this Schedule 6F, the Provider must:

(a) notify the Co-ordinating Commissioner in writing of the intended Sub-processor and processing;

(b) obtain the written consent of the Co-ordinating Commissioner;

(c) carry out appropriate due diligence of the Sub-processor and ensure this is documented;

(d) 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 21.19.2; and

(e) provide the Co-ordinating Commissioner with such information regarding the Sub-processor as the Co-ordinating Commissioner may reasonably require.

***[Drafting Note**: We have not included the wording from the PPN that enables the data controller (Co-ordinating Commissioner) to introduce standard clauses into the data processing agreement or vary the agreement to take account of new ICO guidance. This is because the national contract variation already provides a mechanism for this.]*

2.12 The Provider must create and maintain a record of all categories of data processing activities carried out under this Schedule 6F, containing:

(a) the categories of processing carried out under this Schedule 6F;

(b) 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;

(c) a general description of the Protective Measures taken to ensure the security and integrity of the Personal Data processed under this Schedule 6F; and

(d) a log recording the processing of the Processor Data by or on behalf of the Provider 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.

2.13 The Provider warrants and undertakes that it will deliver the Data Processing Services in accordance with all Data Protection Legislation and this 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.

2.14 The Provider must comply at all times with obligations equivalent to those imposed on the Co-ordinating Commissioner 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.

2.15 The Provider must assist 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 Provider.

2.16 The Provider must take prompt and proper remedial action regarding any Data Loss Event.

2.17 The Provider must assist the Co-ordinating Commissioner by taking appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Commissioners' obligation 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 Provider must comply with any further written instructions with respect to processing by the Co-ordinating Commissioner.

2. Any such further instructions shall be incorporated into this Annex.

Description	Details
Subject matter of the processing	*[This should be a high level, short description of what the processing is about i.e. its subject matter]*
Duration of the processing	*[Clearly set out the duration of the processing including dates]*
Nature and purposes of the 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), Co-ordinating 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 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 the following words and phrases have the following meanings:

Data Processing Services the data processing services described in Annex A to 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 Provider under this Contract or Personal Data for which the Provider has responsibility under this 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 Provider 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

First published: March 2018 (draft)
Published in electronic format only