Template document for the Data Protection Protocol to be used by Participating Authorities when placing Orders (as referred to the in the definition of Data Protection Protocol under the call-off terms and conditions)

* 1. **COVER NOTES**
  2. As part of the January 2018 update, the standard NHS Terms and Conditions for the supply of goods and the provision of services have been updated to reflect the coming into force of the General Data Protection Regulation (**GDPR**). Please see the relevant Crown Commercial Service Procurement Policy Notice (**PPN**) and related model clauses (Changes to Data Protection Legislation & General Data Protection Regulation) here: <https://www.gov.uk/government/publications/procurement-policy-note-0317>).
  3. As part of this update, the Department of Health and Social Care’s policy approach has been to:

1. Adopt the Crown Commercial Service PPN model clauses with only minor changes to ensure consistent use of terminology with the NHS terms and conditions. This has been achieved by developing the Data Protection Protocol below containing such model clauses for completion in connection with relevant Contracts where the Supplier will be processing personal data on behalf of the Authority. Schedule 3 (Information and Data Provisions) of the NHS terms and conditions has been amended to refer to this Protocol accordingly;

2. Make any necessary changes to relevant definitions in the NHS Terms and Conditions to refer to the GDPR and to ensure consistency with the Protocol; and

3. Make some very limited changes to other Clauses as necessary to ensure consistency with the Protocol and to ensure that the Protocol is referred to as appropriate. For example, depending on the version being used, as well as changes to Schedule 3, there are changes to the Supplier as data processor provisions in Schedule 1 (Key Provisions), the consequences of expiry or earlier termination provisions in Schedule 2 (General Terms and Conditions) and the change management provisions in Schedule 2. This Protocol can also be used when varying existing Contracts to comply with the GDPR in circumstances where the Supplier is processing personal data on behalf of the Authority. In these circumstances, a change note will need to be agreed in compliance with the Contract change provisions to replace the existing data protection provisions (e.g. paragraph 2.2 of Schedule 3 in the standard NHS Terms and Conditions) with a completed version of the Protocol (which can be annexed to the change note accordingly). The consequential changes, as referred to at points 2 and 3 above, will also be relevant to any such change notes and can be viewed as part of the comparison documents published as part of the January 2018 update.

* 1. Whether a new or existing Contract, the Protocol should be completed and/or tailored to reflect the actual data processing activities taking place. In the context of more complex data sharing arrangements, for example, the Protocol will need more substantial changes and tailoring to reflect any data controlled by the Supplier and processed by the Authority and/or any data shared with third parties as part of such arrangements.
  2. *Developed in partnership with*
  3. **January 2018**
  4. **DATA PROTECTION PROTOCOL**

*Guidance: This Data Protection Protocol is for use alongside the NHS terms and conditions where the Supplier will be processing personal data on behalf of the Authority. In these circumstances, the table below should be completed by the Authority setting out the nature of the processing that will be taking place under the Contract. This Protocol is based on the model provisions set out in the Procurement Policy Note – Changes to Data Protection Legislation and General Data Protection Regulation (PPN 03/17) issued by the Crown Commercial Service (December 2017).*

* + 1. **Table A – Processing, Personal Data and Data Subjects**

|  |  |
| --- | --- |
| **Description** | **Details** |
| Subject matter of the  Processing | Processing of personal and clinical data for the purpose of dispensing and delivering pharmaceutical products with or without associated clinical services |
| Duration of the  Processing | Duration of processing shall start on the Commencement Date and continue for the Term of the agreement. |
| Nature and purposes of  the Processing | The nature of the processing means any operation such as collection, recording, storage, adaptation or alteration, re consultation, use.  The purpose might include: dispensing and delivering pharmaceutical products with or without associated clinical services  *See attached* |
| Type of Personal Data | *See attached* |
| Categories of Data  Subject | Patients, Carers, Parents, Guardians, Authority and Supplier Clinical and Pharmacy Staff. |
| 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 | <https://www.sps.nhs.uk/articles/retention-of-pharmacy-records/> |

* 1. **Definitions**

1. The definitions and interpretative provisions at Schedule 4 (Definitions and Interpretations) of the Contract shall also apply to this Protocol. Additionally, in this Protocol the following words shall have the following meanings unless the context requires otherwise:

|  |  |
| --- | --- |
| 1. “Data Loss Event” | 1. means any event that results, or may result, in unauthorised access to Personal Data held by the Supplier under this Contract, and/or actual or potential loss and/or destruction of Personal Data in breach of this Contract, including any Personal Data Breach; |
| 1. “**Data Protection Impact Assessment**” | 1. means an assessment by the Controller of the impact of the envisaged Processing on the protection of Personal Data; |
| 1. “**Data Protection Officer**” and **“Data Subject**” | 1. shall have the same meanings as set out in the GDPR; |
| 1. “**Data Recipient**” | 1. means the Controller who agrees to receive Personal Data from the Data Transferor for further Processing in accordance with this Protocol |
| 1. “Data Subject Access Request” | 1. means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data. |
| 1. “**Data Transferor**” | 1. means that controller who transfers the relevant Personal Data. |
| 1. “**Personal Data Breach**” | 1. shall have the same meaning as set out in the GDPR; |
| 1. “Protective Measures” | 1. means 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 adopted by it; |
| 1. “Protocol” or “Data Protection Protocol” | 1. means this Data Protection Protocol; |
| 1. “Sub-processor” | 1. means any third party appointed to Process Personal Data on behalf of the Supplier related to this Contract. |

1. DATA PROCESSING
   1. The Parties acknowledge that the nature of the Services will require the Authority to act as the Controller and the Supplier to act as the Processor. Where such relationship applies:
      1. the only Processing that the Supplier is authorised to do is listed in Table A of this Protocol by the Authority and may not be determined by the Supplier; and
      2. this Clause 1 shall apply.
   2. The Supplier shall notify the Authority immediately if it considers that any of the Authority's instructions infringe the Data Protection Legislation.
   3. The Supplier shall provide all reasonable assistance to the Authority in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Authority, 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 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 Supplier shall, in relation to any Personal Data Processed in connection with its obligations under this Contract:
      1. process that Personal Data only in accordance with Table A of this Protocol, unless the Supplier is required to do otherwise by Law. If it is so required the Supplier shall promptly notify the Authority 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 Authority 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. the Supplier Personnel do not Process Personal Data except in accordance with this Contract (and in particular Table A of this Protocol);
         2. it takes all reasonable steps to ensure the reliability and integrity of any Supplier Personnel who have access to the Personal Data and ensure that they:
            1. are aware of and comply with the Supplier’s duties under this Protocol;
            2. are subject to appropriate confidentiality undertakings with the Supplier or any 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 Authority or as otherwise permitted by this Contract; and
            4. have undergone adequate training in the use, care, protection and handling of Personal Data;
      4. not transfer Personal Data outside of the EU unless the prior written consent of the Authority has been obtained and the following conditions are fulfilled:
         1. the Authority or the Supplier has provided appropriate safeguards in relation to the transfer (whether in accordance with Article 46 of the GDPR or Article 37 of the Law Enforcement Directive (Directive (EU) 2016/680)) as determined by the Authority;
         2. the Data Subject has enforceable rights and effective legal remedies;
         3. the Supplier 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 Authority in meeting its obligations); and
         4. the Supplier complies with any reasonable instructions notified to it in advance by the Authority with respect to the Processing of the Personal Data;
      5. at the written direction of the Authority, delete or return Personal Data (and any copies of it) to the Authority on termination or expiry of the Contract unless the Supplier is required by Law to retain the Personal Data.
   5. Subject to Clause 1.6 of this Protocol, the Supplier shall notify the Authority immediately if 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 either Party's obligations under the Data Protection Legislation;
      4. receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under this Contract;
      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; or
      6. becomes aware of a Data Loss Event.
   6. The Supplier’s obligation to notify under Clause 1.5 of this Protocol shall include the provision of further information to the Authority in phases, as details become available.
   7. Taking into account the nature of the Processing, the Supplier shall provide the Authority with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under Clause 1.5 of this Protocol (and insofar as possible within the timescales reasonably required by the Authority) including by promptly providing:
      1. the Authority with full details and copies of the complaint, communication or request;
      2. such assistance as is reasonably requested by the Authority to enable the Authority to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
      3. the Authority, at its request, with any Personal Data it holds in relation to a Data Subject;
      4. assistance as requested by the Authority following any Data Loss Event;
      5. assistance as requested by the Authority with respect to any request from the Information Commissioner’s Office, or any consultation by the Authority with the Information Commissioner's Office.
   8. The Supplier shall maintain complete and accurate records and information to demonstrate its compliance with this Protocol. This requirement does not apply where the Supplier employs fewer than 250 staff, unless:
      1. the Authority determines that the Processing is not occasional;
      2. the Authority 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; and
      3. the Authority determines that the Processing is likely to result in a risk to the rights and freedoms of Data Subjects.
   9. The Supplier shall allow for audits of its Processing activity by the Authority or the Authority’s designated auditor.
   10. The Supplier shall designate a Data Protection Officer if required by the Data Protection Legislation.
   11. Before allowing any Sub-processor to Process any Personal Data related to this Contract, the Supplier must:
       1. notify the Authority in writing of the intended Sub-processor and Processing;
       2. obtain the written consent of the Authority;
       3. enter into a written agreement with the Sub-processor which give effect to the terms set out in this Protocol such that they apply to the Sub-processor; and
       4. provide the Authority with such information regarding the Sub-processor as the Authority may reasonably require.
   12. The Supplier shall remain fully liable for all acts or omissions of any Sub-processor.
   13. The Authority may, at any time on not less than 30 Business Days’ notice, revise this Protocol 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 this Contract).
   14. The Parties agree to take account of any guidance issued by the Information Commissioner’s Office. The Authority may on not less than 30 Business Days’ notice to the Supplier amend this Protocol to ensure that it complies with any guidance issued by the Information Commissioner’s Office.
   15. The Supplier shall comply with any further instructions with respect to Processing issued by the Authority by written notice. Any such further written instructions shall be deemed to be incorporated into Table A above from the date at which such notice is treated as having been received by the Supplier in accordance with Clause 27.2 of Schedule 2 of the Contract.
   16. Subject to Clauses 1.13, 1.14, and 1.15 of this Protocol, any change or other variation to this Protocol shall only be binding once it has been agreed in writing and signed by an authorised representative of both Parties.
   17. In the event that the Supplier acting as a Controller engages the Authority as a Processor, the Parties shall agree the terms of that processing on similar terms to those set out in this Clause 1.
2. BOTH DATA CONTROLLERS
   1. To the extent that the nature of the Services means that the Parties are acting both as Controllers, each Party undertakes to comply at all times with its obligations under the Data Protection Legislation and shall:
      1. implement such measures and perform its obligations (as applicable) in compliance with the Data Protection Legislation;
      2. be responsible for determining its data security obligations taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing as well as the risk of varying likelihood and severity for the rights and freedoms of the Data Subjects, and implement appropriate technical and organisational measures to protect the Personal Data against unauthorised or unlawful processing and accidental destruction or loss and ensure the protection of the rights of the Data Subject, in such a manner that processing will meet the requirements of the Data Protection Legislation where Personal Data has been transmitted by it, or while the Personal Data is in its possession or control;
      3. where appropriate, promptly refer to the other Party any requests, from (i) Data Subjects in regards to the right of access to Personal Data by that Data Subject in accordance with the Data Protection Legislation; (ii) the Information Commissioner; or (iii) any other law enforcement authority and to the extent it is reasonable and practical to do so consult with the other Party (for the avoidance of doubt at no additional cost) before responding to such request.
   2. Where Personal Data is shared between the Parties, each acting as Controller:
      1. the Data Transferor warrants and undertakes to the Data Recipient that such Personal Data have been collected, processed and transferred in accordance with the Data Protection Legislation and this Clause 2;
      2. the Data Recipient will process the Personal Data in accordance with the Data Protection Legislation and this Clause 2; and
      3. where the Data Recipient is in breach of its obligations under this Protocol and the Data Protection Legislation, the Data Transferor may temporarily suspend the transfer of the Personal Data to the Data Recipient until the breach is repaired.

Clinical Referring Centre

Homecare Provider

Patient

Registration Form   
*(new pts)*

Prescription Form

Consent Form\*  
*(new pts)*

Direct patient contact:   
[Non] Clinical Delivery Scheduling call  
[+Welcome call &pack for new pts]

Product / Service Delivered

Signature obtained for Proof of Delivery/Clinical Service Report

Proof of Delivery

Clinical Service Report

Invoice

Repeat Prescription Request

Clinical service report added to patient notes

Invoice validated & passed for payment

Prescription Form

Individual Care Plan *(where req.)*

\*Provided in welcome pack if not completed with registration

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Data Transaction** | **From** | **To** | **Personal Data fields** *(Note: additional data may be captured which is not, in itself, Personal Data as defined in GDPR)* | **Mandatory / optional** | **Data Controller** | **Data Processor** | **Comments** |
| Registration Form  [Written] | CRC | HCP | Designation | Opt | CRC | HCP |  |
| CRC | HCP | Full Name | Man | CRC | HCP |  |
| CRC | HCP | Date of Birth | Man | CRC | HCP |  |
| CRC | HCP | NHS Number | Opt | CRC | HCP | (NHS or Hospital no. mandatory) National patient identifier |
| CRC | HCP | Hospital number | Opt | CRC | HCP | (NHS or Hospital no. mandatory) Clinical referring centre patient identifier |
| CRC | HCP | Home Address | Man | CRC | HCP |  |
| CRC | HCP | Delivery Address | Opt | CRC | HCP | (Non)Clinical service delivery address If not home address |
| CRC | HCP | Authorised Signatory(ies) | Opt | CRC | HCP | If not the patient |
| CRC | HCP | Preferred telephone Number | Man | CRC | HCP |  |
| CRC | HCP | Alternative / mobile telephone Number | Opt | CRC | HCP |  |
| CRC | HCP | Email | Opt | CRC | HCP |  |
| CRC | HCP | Service area | Man | CRC | HCP |  |
| CRC | HCP | Diagnosis | Opt | CRC | HCP |  |
| CRC | HCP | Carer / Parent / Guardian Name | Opt | CRC | HCP |  |
| CRC | HCP | Carer / Parent / Guardian Telephone | Opt | CRC | HCP |  |
| CRC | HCP | Clinical service requirements | Opt | CRC | HCP |  |
| CRC | HCP | Clinician Name | Man | CRC | HCP |  |
| CRC | HCP | Clinician Telephone | Man | CRC | HCP |  |
| CRC | HCP | Clinician Email | Man | CRC | HCP |  |
| CRC | HCP | Clinical Pharmacist Name | Opt | CRC | HCP |  |
| CRC | HCP | Clinical Pharmacist Telephone | Opt | CRC | HCP |  |
| CRC | HCP | Clinical Pharmacist Email | Opt | CRC | HCP |  |
| CRC | HCP | Pharmacy Homecare Lead name | Opt | CRC | HCP |  |
| CRC | HCP | Pharmacy Homecare Lead Telephone | Opt | CRC | HCP |  |
| CRC | HCP | Pharmacy Homecare Lead Email | Opt | CRC | HCP |  |
| CRC | HCP | Contact email for repeat prescriptions | Opt | CRC | HCP |  |
| Consent Form  [Written] | CRC | HCP | Designation | Opt | CRC | HCP |  |
| CRC | HCP | Full Name | Man | CRC | HCP |  |
| CRC | HCP | NHS Number | Opt | CRC | HCP | (NHS or Hospital no. mandatory) National patient identifier |
| CRC | HCP | Hospital number | Opt | CRC | HCP | (NHS or Hospital no. mandatory) Clinical referring centre patient identifier |
|  | CRC | HCP | Carer / Parent / Guardian Name | Opt | CRC | HCP |  |
| Prescription Form  [Written] | CRC | HCP | Designation | Opt | CRC/HCP\* | HCP | \*As a registered pharmacy HCP must retain prescription and dispensing record |
| CRC | HCP | Full Name | Man | CRC/HCP | HCP |  |
| CRC | HCP | Date of Birth | Man | CRC/HCP | HCP |  |
| CRC | HCP | NHS Number | Opt | CRC/HCP | HCP | (NHS or Hospital no. mandatory) National patient identifier |
| CRC | HCP | Hospital number | Opt | CRC/HCP | HCP | (NHS or Hospital no. mandatory) Clinical referring centre patient identifier |
| CRC | HCP | Home Address | Man | CRC/HCP | HCP |  |
| CRC | HCP | Purchase order Number | Man | CRC/HCP | HCP | Indirect patient identifier with 1:1 PO:Rx relationship |
| CRC | HCP | Prescribed Medicine(s) | Man | CRC/HCP | HCP |  |
| CRC | HCP | Dosage instructions | Man | CRC/HCP | HCP |  |
| CRC | HCP | Allergy information | Man | CRC/HCP | HCP |  |
| CRC | HCP | Blood test results (or similar) | Opt | CRC/HCP | HCP |  |
|  | CRC | HCP | Prescriber Name | Man | CRC/HCP | HCP |  |
|  | CRC | HCP | Prescriber Registration Number | Man | CRC/HCP | HCP |  |
|  | CRC | HCP | Pharmacist Name | Opt | CRC/HCP | HCP |  |
|  | CRC | HCP | Pharmacist Signature | Opt | CRC/HCP | HCP |  |
| Individual care plan  [Written] | CRC | HCP | Designation | Opt | CRC | HCP |  |
| CRC | HCP | Full Name | Man | CRC | HCP |  |
| CRC | HCP | Date of Birth | Man | CRC | HCP |  |
| CRC | HCP | NHS Number | Opt | CRC | HCP | (NHS or Hospital no. mandatory) National patient identifier |
| CRC | HCP | Hospital number | Opt | CRC | HCP | (NHS or Hospital no. mandatory) Clinical referring centre patient identifier |
| CRC | HCP | Home Address | Man | CRC | HCP |  |
| CRC | HCP | Special care requirements | Man | CRC | HCP |  |
| Invoice  [Written] | HCP | CRC | Purchase order Number | Man | CRC | HCP | Indirect patient identifier with 1:1 PO:Rx relationship |
| Proof of Delivery  [Written] | HCP | CRC | Patient / Authorised Signatory Name | Man | CRC | HCP |  |
| HCP | CRC | Patient / Authorised Signatory Signature | Man | CRC | HCP |  |
| HCP | CRC | Delivery Address | Man | CRC | HCP |  |
| HCP | CRC | Purchase order Number | Man | CRC | HCP |  |
| HCP | CRC | Supplier patient number | Opt | HCP |  | Supplier patient identifier |
|  | HCP | CRC | Delivery Driver Name | Opt | HCP/CRC |  |  |
| Clinical service report (inc. training progress, competency assessment, administration/exception report)  [Written] | HCP | CRC | Designation | Opt | CRC | HCP |  |
| HCP | CRC | Full Name | Man | CRC | HCP |  |
| HCP | CRC | Date of Birth | Man | CRC | HCP |  |
| HCP | CRC | NHS Number | Opt | CRC | HCP | (NHS or Hospital no. mandatory) National patient identifier |
| HCP | CRC | Hospital number | Opt | CRC | HCP | (NHS or Hospital no. mandatory) Clinical referring centre patient identifier |
| HCP | CRC | Supplier patient number | Opt | HCP |  |  |
| HCP | CRC | Home Address | Man | CRC | HCP |  |
| HCP | CRC | Delivery Address | Opt | CRC | HCP | Only where issued by Clinical referring centre on registration form |
| HCP | CRC | Home suitability assessment details | Opt | CRC/HCP |  |  |
| HCP | CRC | Competency assessment details | Opt | CRC/HCP |  |  |
| HCP | CRC | Summary of clinical service undertaken | Opt | CRC/HCP |  |  |
| HCP | CRC | Summary of exceptions to prescribed service | Opt | CRC/HCP |  |  |
| HCP | CRC | Nurse (or other clinician) Name | Man | CRC/HCP |  |  |
| Repeat Prescription Request  [Written] | CRC | HCP | Designation | Opt | CRC | HCP |  |
| CRC | HCP | Full Name | Opt | CRC | HCP |  |
| CRC | HCP | Date of Birth | Man | CRC | HCP |  |
| CRC | HCP | NHS Number | Opt | CRC | HCP | (NHS or Hospital no. mandatory) National patient identifier |
| CRC | HCP | Hospital number | Opt | CRC | HCP | (NHS or Hospital no. mandatory) Clinical referring centre patient identifier |
| CRC | HCP | Service Area | Opt | CRC | HCP |  |
| Direct patient contact  [Verbal or written] | HCP | PT | Designation | Opt | HCP | HCP |  |
| HCP | PT | NHS Number | Opt | HCP | HCP |
| HCP | PT | Hospital number | Opt | HCP | HCP |
| HCP | PT | Delivery Address | Opt | HCP | HCP |
| HCP | PT | Authorised Signatory(ies) | Opt | CRC | HCP |
| HCP | PT | Alternative / mobile telephone Number | Opt | HCP | HCP |
| HCP | PT | Email | Opt | HCP | HCP |
| HCP | PT | Other patient identifier | Opt | HCP | HCP |

Key:  
CRC = Clinical Referring Centre  
HCP = Homecare Provider  
PT = Patient