Part 1: Front Sheet

IG Reference: 

Contract Reference: 

1. This Data Sharing Framework Contract (Contract) comprises this Part 1 (Front Sheet), Part 2 (Terms and Conditions) and the Schedules. It sets out the terms on which the HSCIC agrees to share the Data with the Data Recipient.

2. This Contract is made between:

**The Health & Social Care Information Centre (HSCIC),** a body corporate established pursuant to section 252 of the Health and Social Care Act 2012 whose address is 1 Trevelyan Square, Boar Lane, Leeds LS1 6AE; and

The party whose details are set out below (the Data Recipient):

| Name: |  |
| Company Number (if relevant): |  |
| Address: |  |

3. The purpose of this Contract is to:
   - clarify the responsibilities of the parties in relation to the Data;
   - outline the data security principles and requirements with which the Data Recipient must comply;
   - set out the audit rights of the HSCIC;
   - impose confidentiality requirements on the Data Recipient; and
   - include arrangements for termination of this Contract.

4. The term of this Contract shall be:

| Start Date | [dd/mm/yyyy] | End Date | [dd/mm/yyyy] |
| Term: | 3 years |

5. No Data will be shared directly under this Contract. Each time the Data Recipient wishes to receive Data, a Data Sharing Agreement (DSA) will be completed and signed by the Parties. Each DSA will incorporate the terms of this Contract. In no circumstances will a DSA be agreed without the parties first entering into this Contract.

6. Each DSA will include details of:
   - the Data to be provided;
   - the legal basis for sharing Data;
   - the purpose of the sharing and use of the Data;
• the method of transfer;
• any special terms and conditions for the use or reuse of the Data; and
• any Charges payable for the provision of the Data.

7 If there is a conflict or inconsistency between any provision contained in Part 1 (Front Sheet), Part 2 (Terms and Conditions) and the Schedules, the provisions of this Part 1 shall prevail, then Part 2, then the Schedules.

By signing this Part 1, the parties agree to be bound by the terms of this Contract.

Signed for and on behalf of the **Data Recipient**:

<table>
<thead>
<tr>
<th>Organisation Name:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature:</td>
<td></td>
</tr>
<tr>
<td>Name:</td>
<td></td>
</tr>
<tr>
<td>Position in organi</td>
<td></td>
</tr>
<tr>
<td>[Caldicott Guardian/SIRO/senior executive or equivalent]</td>
<td></td>
</tr>
<tr>
<td>Date:</td>
<td>[dd/mm/yyyy]</td>
</tr>
</tbody>
</table>

Signed for and on behalf of the **Health and Social Care Information Centre**:

<table>
<thead>
<tr>
<th>Name:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature:</td>
<td></td>
</tr>
<tr>
<td>Role:</td>
<td>[Caldicott Guardian/SIRO/ Executive Director]</td>
</tr>
<tr>
<td>Date:</td>
<td>[dd/mm/yyyy]</td>
</tr>
</tbody>
</table>
Part 2: Terms and Conditions

1 Interpretation
1.1 Capitalised words and expressions used in this Contract shall bear the meanings given to them in Schedule 1. The rules of interpretation set out in Schedule 1 shall apply to this Contract.

2 HSCIC responsibilities
2.1 The HSCIC will transfer the Data to the Data Recipient (or, if specified in the DSA, the data processor authorised by the HSCIC) using the data transfer method as set out in the relevant DSA.
2.2 The HSCIC is a Data Controller, or is acting on behalf of the Data Controller, for the Data insofar as the Data constitutes Personal Data.

3 Licence and Intellectual Property
3.1 The HSCIC grants to the Data Recipient a non-exclusive, revocable licence to use the Data in the Territory for the duration of the term of the relevant DSA solely for the Purpose and only in accordance with this Contract and the relevant DSA.
3.2 The Data Recipient shall not be entitled to sub-license the Data unless:
   3.2.1 the HSCIC has specifically authorised such sub-licensing in the DSA;
   3.2.2 the Data Recipient complies at all times with the sub-licensing conditions set out in the DSA, which shall be in the form set out in Schedule 5; and
   3.2.3 the Data Recipient has entered into an agreement with any sub-licensee for the sub-licensing of the Data which contains provisions which are, as a minimum, equivalent to those set out in this Contract and the DSA.
3.3 The Intellectual Property Rights in the Data and any derivative works shall remain at all times the property of the HSCIC. All rights in the Data not expressly granted under the relevant DSA are reserved to the HSCIC.
3.4 The Data Recipient must cite the HSCIC’s copyright correctly as follows: "Copyright © <year>, re-used with the permission of The Health & Social Care Information Centre. All rights reserved."
3.5 The Data Recipient shall ensure that any publication derived from the Data by any party complies with the following guidance:
   3.5.1 Anonymisation Standard for Publishing Health and Social Care Data: http://www.isb.nhs.uk/library/standard/128; and
3.6 Where the Data derives from the Office for National Statistics, the Data Recipient must also comply with the following guidance:

4 Data Recipient responsibilities
4.1 Where the Data Recipient obtains Data from the HSCIC:
4.1.1 if the Data constitutes Personal Data, the Data Recipient shall hold the Data as a Data Controller (either alone or in common or jointly with the HSCIC, as specified in the DSA); or

4.1.2 if the Data constitutes Non-Identifiable Data, but then the Data becomes Personal Data in the hands of the Data Recipient, the Data Recipient shall become a Data Controller.

4.2 Where the Data Recipient obtains Data from the HSCIC that does not constitute Personal Data, the Data is not subject to the requirements of the DPA. However, the Data Recipient shall be responsible for processing such Data in accordance with all Applicable Laws and all regulatory standards applicable to such Data;

4.3 The Data Recipient shall:

4.3.1 use the Data only in accordance with the Purpose;

4.3.2 process the Data only in accordance with the terms of this Contract and the relevant DSA, including any Special Conditions contained in the DSA;

4.3.3 not share the Data with any third party without the prior written consent of the HSCIC;

4.3.4 ensure that staff processing the Data are suitably trained and made aware of their responsibilities in handling the Data;

4.3.5 subject to Clause 13, on termination of this Contract, the relevant DSA or earlier if use of the Data is completed, destroy the Data, together with all hard or soft copies of the same and certify such destruction to the HSCIC;

4.3.6 notify any Data Breach to the HSCIC as soon as the Data Recipient discovers such Data Breach and assess whether a Serious Incident Requiring Investigation (SIRI) report needs to be made, as mandated by the Information Governance Toolkit. Such assessment must include whether or not to report the Data Breach to the Information Commissioner;

4.3.7 immediately notify the HSCIC if it no longer has a legal basis on which to process the Data.

4.4 Unless specified in the Purpose or otherwise authorised by the HSCIC, the Data Recipient must not combine the Data with any other data held by the Data Recipient and must not seek to re-identify any individual from the Data.

4.5 If the Data Recipient is obliged to respond to requests under the Freedom of Information Act 2000 and a request is received regarding the Data, the Data Recipient must consult with the HSCIC prior to any release of Data.

4.6 The Data Recipient shall comply at all times with:

4.6.1 the Data Security Requirements set out in Schedule 2; and

4.6.2 the DPA (to the extent that the Data includes Personal Data or becomes Personal Data in the hands of the Data Recipient), the common law duty of confidentiality and all other Applicable Law and Department of Health directives covering issues of data sharing, including but not limited to those listed in Schedule 3.

4.7 Before undertaking any Publishing activity using the Data or any derived information, the Data Recipient will undertake an organisational risk assessment exercise to ensure compliance with the terms of this Contract and the relevant DSA. The Data Recipient shall conduct the risk assessment in accordance with the standards set out in the Anonymisation Standard for Publishing Health and Social Care Data.

5 Data protection

5.1 To the extent that any of the Data constitutes Personal Data, the Data Recipient shall process such Data at all times:
5.1.1 in accordance with the DPA; and
5.1.2 using appropriate technical and organisational security measures against unauthorised or unlawful processing of Data and against accidental loss or destruction of, or damage to, the Data.

5.2 The Data Recipient shall not transfer Personal Data to another territory outside the European Economic Area except with the express prior written consent of the HSCIC and only in circumstances when such transfer is permitted under the DPA.

5.3 Where the Data includes Personal Data, the Data Recipient shall:

5.3.1 store and process the Data securely, and destroy it when it is no longer needed for the Purpose;
5.3.2 not publish the Data without the prior written consent of the HSCIC. In deciding whether to give its consent, the HSCIC shall consider whether the Data has been de-identified to a standard suitable for subsequent release in compliance with the Anonymisation Standard for Publishing Health and Social Care Data;
5.3.3 maintain good information governance standards and practices, meeting or exceeding the Information Governance Toolkit standards required of its organisation type;
5.3.4 not disseminate the Data, or a subset of the Data, to other bodies without prior written consent from the HSCIC;
5.3.5 take reasonable steps to ensure the reliability of each of its Personnel who have access to the Personal Data;
5.3.6 inform the HSCIC immediately if it receives any communication from the Information Commissioner's Office which relates to the Personal Data; and
5.3.7 ensure access to the Data is managed, auditable and restricted to those needing to process the Data.

5.4 The Data Recipient must not contact any individual that could be identified from the information supplied, except with the prior written consent of the individual concerned, and the prior written consent of the HSCIC. In determining whether to grant such consent, the HSCIC will consider the statutory authority and the public interest, having regard to guidance published by the Department of Health, NHS England or the HSCIC.

5.5 In the event of any change in data protection laws subsequent to the date of signature of this Contract, the Data Recipient shall take such steps (including, agreeing to additional obligations and/or executing additional documents) as may be requested by the HSCIC to ensure that the transfer to the Data Recipient, and the processing by the Data Recipient, of the Personal Data complies with such data protection laws.

5.6 The Data Recipient may only appoint a data processor to process the Data on behalf of the Data Recipient with the prior written consent of the HSCIC.

6 Confidentiality

6.1 The Data Recipient must:

6.1.1 keep the Data separate from all other information and shall keep such information confidential and shall not disclose it to any third party or make any attempts to identify an individual from the Data save where expressly permitted to do so in accordance with the terms of this Contract and the relevant DSA; and
6.1.2 use the Data only in so far as is necessary to perform its obligations under this Contract and the relevant DSA.

6.2 The restrictions on disclosure and use contained in this Clause 6 shall not apply to information to the extent that it is or was:
6.2.1 already in the possession of or becomes available to Data Recipient in either case free of any obligation of confidentiality;
6.2.2 is required to be disclosed by the Data Recipient by law, regulation or pursuant to an order of a competent authority, or to a professional adviser; or
6.2.3 at the time of receipt by the Data Recipient, is in the public domain or after such receipt comes into the public domain other than as a result of breach by the Data Recipient of this Clause 6.

6.3 The Data Recipient shall be responsible for any unauthorised disclosure or use of the Data made by any of its Personnel and shall take all reasonable precautions to prevent such unauthorised disclosure or use.

6.4 The confidentiality obligations contained in this Clause 6 shall continue indefinitely following termination or expiry of this Contract and any DSA to which the Data relates.

7 Audit and specific rights
The HSCIC shall be entitled at any time during the term of this Contract to audit the Data Recipient’s use of the Data. The Data Recipient shall, for the purpose of such audit, provide or procure the access to the Data Recipient’s sites, systems, procedures, documents and staff as may be necessary or desirable in connection with the audit and shall permit the HSCIC to take copies of relevant documents and data pursuant to such audit. The Data Recipient shall provide such information as the HSCIC reasonably requests in order to verify its compliance with the terms of this Contract and any DSA.

8 Warranties
8.1 The Data Recipient warrants that:
8.1.1 it has the full right and authority to enter into this Contract;
8.1.2 it shall use the Data in accordance with all Applicable Laws.

8.2 The Data is provided to the Data Recipient by the HSCIC on an ‘as is’ basis and the HSCIC does not warrant the accuracy or completeness of the Data, nor that the Data does not infringe the Intellectual Property Rights of any third party, nor does it undertake that the Data will meet the requirements of or be fit for purpose of the Data Recipient.

9 Charges
9.1 In consideration of the provision of the Data by the HSCIC, the Data Recipient agrees to pay the Charges (if any) as set out in the applicable DSA. All Charges payable are exclusive of value added tax and all other applicable taxes, duties of levies.

9.2 Charges shall be paid within 30 days of the date of the HSCIC’s invoice.

10 Liability
10.1 This Clause 10 sets out the entire liability of the HSCIC to the Data Recipient in respect of:
10.1.1 any breach by the HSCIC of this Contract and/or any DSA;
10.1.2 negligence for which the HSCIC is liable or any other tortious liability or breach of statutory duty in connection with this Contract and/or any DSA; and
10.1.3 any representation or statement arising under or in connection with this Contract and/or any DSA or by or on behalf of the HSCIC.

10.2 Subject to Clause 10.5, the HSCIC shall in no circumstances be liable to the Data Recipient for:
10.2.1 any loss of profits, revenue, opportunity, contracts, sales, turnover, anticipated savings, goodwill, reputation, business opportunity, production, or loss to or corruption of data (regardless of whether any of these losses or damages are direct, indirect or consequential); and
10.2.2 any Indirect Loss.

10.3 Other than any warranties expressly set out in this Contract, all warranties, conditions or other terms, whether express or implied by statute, common law, trade usage or otherwise are excluded except to the extent the exclusion is prohibited by law.

10.4 [Liability TBC]

10.5 Nothing in this Contract shall limit the HSCIC's liability to the Data Recipient for:

10.5.1 death or personal injury resulting from the negligence of the HSCIC, its employees, agents or subcontractors; or

10.5.2 fraud or fraudulent misrepresentation; or

10.5.3 any other liability that cannot be excluded or limited as a matter of law.

11 Indemnity

The Data Recipient shall indemnify the HSCIC in full for any liabilities, losses, demands, claims, damages, amounts agreed in settlement, costs and expenses incurred which arise from or in connection with the Data Recipient's loss of the Data, unauthorised or unlawful use of the Data or any breach of this Contract whether arising in negligence, contract or otherwise and including any monetary penalty notice imposed on the HSCIC by the Information Commissioner under Section 55 of the DPA.

12 Term and termination

12.1 This Contract shall, subject to prior termination in accordance with this Clause 12, continue for the period set out in Part 1.

12.2 Subject to prior termination under Clause 12.3, the HSCIC may terminate this Contract and/or any DSA by giving to the Data Recipient not less than one month's prior written notice.

12.3 On or at any time after the occurrence of an event specified in Clause 12.4, the HSCIC shall be entitled to terminate this Contract and/or any DSA, with immediate effect by written notice to the Data Recipient.

12.4 The events are:

12.4.1 the Data Recipient is in material breach of this Contract and/or any DSA and that breach cannot be remedied;

12.4.2 the Data Recipient is in material breach of this Contract and/or any DSA which can be remedied but the Data Recipient fails to do so within 30 days starting on the day after receipt of written notice from the HSCIC;

12.4.3 in respect of Personal Data, the Data Recipient no longer has the legal basis to process this Data;

12.4.4 the Data Recipient stops payment of its debts or is unable to pay its debts as they fall due;

12.4.5 the Data Recipient is dissolved;

12.4.6 the Data Recipient becomes or is declared insolvent or a resolution is passed for the winding up of the Data Recipient or the Data Recipient convenes a meeting of its creditors or makes or proposes to make any arrangement or composition with its creditors or a liquidator, an administrative receiver, a receiver, manager, trustee or administrator or analogous officer is appointed in respect of all or any part of its property, undertaking or assets or the Data Recipient becomes subject to any bankruptcy procedure or analogous insolvency procedure in any jurisdiction or any person files a notice of intention to appoint an administrator or a notice of appointment of an administrator or applies to court for an administration order in respect of the Data Recipient;
12.4.7 it becomes unlawful for the Data Recipient to perform all or any of its obligations under this Contract and/or any DSA;
12.4.8 there is a change in law which materially affects the HSCIC’s powers to provide Data to the Data Recipient; or
12.4.9 the Data Recipient (being a natural person) shall die or become mentally incapacitated.

12.5 Without prejudice to the HSCIC’s rights under Clause 12.3, where the Data Recipient either (i) commits any breach of this Contract and/or any DSA, or (ii) an event specified in Clause 12.4 occurs, the HSCIC shall be entitled to suspend this Contract and/or any DSA without incurring any liability to the Data Recipient, with immediate effect by written notice to the Data Recipient.

12.6 The Data Recipient may terminate the Contract at any time by notifying the HSCIC in writing.

12.7 Termination of this Contract will automatically terminate all DSAs that are entered into under this Contract.

13 Consequences of termination

13.1 Subject to Clause 13.2, on termination or expiry of this Contract or any DSA for any reason, the Data Recipient must ensure that:

13.1.1 all Data is securely destroyed promptly and in any event within 14 days of the date of termination or expiry of this Contract or any DSA; and

13.1.2 confirmation of the destruction is provided to the HSCIC in the form of a Certificate of Destruction.

13.2 The Data Recipient may request that it retains use of the Data following termination or expiry of the DSA. The HSCIC shall in its absolute discretion determine whether to grant such a request. The HSCIC will notify the Data Recipient in writing if it grants permission for the Data Recipient to retain use of the Data, and the terms on which the Data Recipient shall be entitled to continue to use the Data.

14 Assignment

The Data Recipient shall not, without the prior written consent of the HSCIC, assign, novate, transfer, charge, dispose of or deal in any other manner with this Contract and/or any DSA, or any of its rights or beneficial interests under it, or purport to do any of the same, nor sub-contract any or all of its obligations under this Contract. The HSCIC may assign, transfer, charge, dispose of or deal in any manner with its rights and obligations under this Contract and/or any DSA. Where it does so, the HSCIC shall notify the Data Recipient of such change.

15 Notices

15.1 Except where any provision of this Contract states otherwise, all notices and communications sent pursuant to this Contract shall be in writing and shall be deemed to have been duly given:

15.1.1 when delivered, if delivered by hand;

15.1.2 if sent by email, when the sender receives a reply email confirming delivery; or

15.1.3 on the second working day after mailing, first class postage pre-paid.

15.2 Notices shall be addressed to the addresses provided in Part 1 of this Contract or to such other address as the parties may notify in writing from time to time. Each party shall notify the other party in accordance with this Clause 15 if the address specified in Part 1 of this Contract is no longer an appropriate address for the service of notices and communications.

16 Miscellaneous

16.1 Nothing in this Contract or any arrangement contemplated by it shall constitute either party a partner, agent, fiduciary or employee of the other party.
16.2 No amendment or variation of the terms of this Contract shall be effective unless made or confirmed in writing and signed by the parties to this Contract.

16.3 If any provision of this Contract shall be found by any court or body or authority of competent jurisdiction to be invalid or unenforceable, such provision shall be severed from the remainder of this Contract which shall remain in full force and effect to the extent permitted by law.

16.4 The rights and remedies provided by this Contract are cumulative and (unless otherwise provided in this Contract) are not exclusive of any rights or remedies provided by law.

16.5 This Contract does not create, confer or purport to create or confer any benefit or right enforceable by any person not a party to it (except that a person who is a permitted successor to or assignee of the rights of a party to this Contract shall be deemed to be a party to this Contract).

16.6 The HSCIC shall not be liable to the Data Recipient for any delays in performance, non-performance or breach of any of its obligations under this Contract and/or any DSA caused by matters beyond its reasonable control. Such matters shall include (without limitation) industrial disputes, acts of God, insurrection or civil disorder, war or military operations, national or local emergency, acts of government or acts or omissions of third parties.

17 Governing law and jurisdiction

17.1 This Contract and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with English law.

17.2 Each party irrevocably agrees that, subject to Clause 17.3, the courts of England and Wales shall have exclusive jurisdiction to hear and determine any suit, action or proceedings, and to settle any disputes or claims (including non-contractual disputes or claims) which may arise out of or in connection with this Contract and/or any DSA, its subject matter or formation.

17.3 Nothing in this Clause 17 shall limit the right of the HSCIC to take proceedings against the Data Recipient in any other court of competent jurisdiction, nor shall the taking of proceedings in any one or more jurisdictions preclude the taking of proceedings in any other jurisdictions, whether concurrently or not, to the extent permitted by the law of such other jurisdiction.

18 Entire agreement

18.1 This Contract constitutes the entire agreement and understanding of the parties and supersedes any previous agreement between the parties relating to the subject matter of this Contract but without prejudice to the rights and liabilities of the parties accrued before the date of this Contract.

18.2 Nothing in this Clause 18 shall operate to limit or exclude any liability for fraud.
SCHEDULE 1

Interpretation

1. In this Contract the following expressions have the following meanings:

<table>
<thead>
<tr>
<th>Expression</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;Applicable Law&quot;</td>
<td>all laws, regulations, orders, guidance (including codes of practice and guidance issued by the Information Commissioner), directions or determinations that are applicable to the obligations of the Data Recipient under this Contract and/or any DSA;</td>
</tr>
<tr>
<td>&quot;Certification of Destruction&quot;</td>
<td>a certificate signed by an authorised representative of the Data Recipient which certifies that the Data and all hard and soft copies thereof have been securely destroyed by the Data Recipient;</td>
</tr>
<tr>
<td>&quot;Charges&quot;</td>
<td>the charges payable, if any, for the provision of the Data as set out in the relevant DSA/s where applicable;</td>
</tr>
<tr>
<td>&quot;Data&quot;</td>
<td>any data that is provided by HSCIC to the Data Recipient under a DSA;</td>
</tr>
<tr>
<td>&quot;Data Breach&quot;</td>
<td>a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to Data;</td>
</tr>
<tr>
<td>&quot;Data Controller&quot;</td>
<td>a data controller as defined in Section 1(1) of the DPA;</td>
</tr>
<tr>
<td>&quot;DPA&quot;</td>
<td>the Data Protection Act 1998. In the event that the DPA is superseded by another data protection law, the term &quot;DPA&quot; shall be construed to mean the new data protection law, and terms used in this Contract shall be given the corresponding meaning under the new data protection law;</td>
</tr>
<tr>
<td>&quot;Indirect Loss&quot;</td>
<td>any indirect loss, damage, costs or expenses arising out of or in connection with this Contract or its contemplated or lack of performance;</td>
</tr>
<tr>
<td>&quot;Intellectual Property Rights&quot; or &quot;IPR&quot;</td>
<td>all intellectual property rights including copyright, database rights, trade marks and trade names, patents, topography rights, design rights, trade secrets, know-how and all rights of a similar nature or having similar effect which subsist anywhere in the world, whether or not any of them are registered and applications for registrations of any of them;</td>
</tr>
<tr>
<td>&quot;Non-Identifiable Data&quot;</td>
<td>information that does not relate to people including information about organisations, companies, resources, projects or information about people that has been aggregated to a level that is not about individuals but that could become Personal Data when merged with other data sets held by the Data Recipient;</td>
</tr>
<tr>
<td>&quot;Personal Data&quot;</td>
<td>personal data as defined in Section 1(1) of the DPA;</td>
</tr>
<tr>
<td>&quot;Personnel&quot;</td>
<td>all employees, agents and contractors of the Data Recipient</td>
</tr>
<tr>
<td><strong>Data Sharing Framework Contract</strong></td>
<td></td>
</tr>
<tr>
<td>-----------------------------------</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Description</strong></th>
<th><strong>Definition</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>&quot;process&quot; and &quot;processing&quot;</td>
<td>have the meaning set out in section 1(1) of the DPA;</td>
</tr>
<tr>
<td>&quot;Publish&quot;</td>
<td>to make available to third parties in any form, including the production of hard copy materials, soft and/or electronic copies, e-mails and posting online;</td>
</tr>
<tr>
<td>&quot;Purpose&quot;</td>
<td>the purpose(s) for which the Data Recipient is permitted to use the Data, as set out in the relevant DSA;</td>
</tr>
<tr>
<td>&quot;Special Conditions&quot;</td>
<td>the special conditions for processing the Data as set out in the DSAs; and</td>
</tr>
<tr>
<td>&quot;Territory&quot;</td>
<td>the territory specified in the relevant DSA.</td>
</tr>
</tbody>
</table>

2 **In this Contract:**

   2.1 any gender includes any other gender and the singular includes the plural and vice versa;

   2.2 references to persons include bodies corporate, unincorporated associations, governments, states, partnerships and trusts (in each case, whether or not having separate legal personality);

   2.3 the Schedules form part of this Contract and the expression "this Contract" includes the Schedules; and

   2.4 any reference to a statutory provision includes a reference to any modification, consolidation or re-enactment of the provision from time to time in force and all subordinate instruments, orders or regulations made under it.
SCHEDULE 2
Data Security Requirements

Part 1

1. Without prejudice to the Data Recipient’s other obligations in respect of information security, the Data Recipient shall:
   
   1.1 having regard to the state of technological development, provide a level of security (including appropriate technical and organisational measures) appropriate to:
      
      1.2.1 the harm that might result from unauthorised or unlawful processing of Data or accidental loss, destruction or damage of such Data; and
      
      1.2.2 the nature of the Data;
   
   1.2 ensure that access to the Data is limited to those Personnel who need access to the Data to meet the Data Recipient’s obligations under this Contract;
   
   1.3 take reasonable steps to ensure the reliability of the Data Recipient’s Personnel who have access to the Data which shall include:
      
      1.3.1 ensuring all Personnel understand the confidential nature of the Data and the issues which arise if proper care is not taken in the processing of the Data;
      
      1.3.2 ensuring all Personnel are properly trained in data protection and to ensure that all Personnel have completed such training prior to their use of the Data. Where requested to do so the Data Recipient shall provide examples of training materials used, together with methodologies used to demonstrate that Personnel have understood the training. Training shall be repeated at regular intervals to take account of developments in law on good data protection practice and in any event on an annual basis; and
      
      1.3.3 ensuring all Personnel are properly vetted, both during the initial recruitment process and throughout their engagement in their processing of the Data, including through the use of procedures to identify changes in personal circumstances which may affect an individual’s ability to process the Data in accordance with the terms of this Contract;
   
   1.4 provide the HSCIC with such information, assistance and co-operation as the HSCIC may require from time to time to establish the HSCIC’s and/or the Data Recipient’s compliance with the DPA;
   
   1.5 inform the HSCIC as soon as reasonably practicable of any particular risk to the security of the DPA of which it becomes aware and of the categories of Data and individuals which may be affected;

2 The Data Recipient shall promptly, and in any event not later than reasonably required in order to enable the HSCIC to fulfil its duties under the DPA:
   
   2.1 pass on to the HSCIC any enquiries or communication (including subject access requests) relating to their Personal Data or its processing; and
   
   2.2 provide such information as may be required for the purpose of responding to any such data subjects or otherwise to comply with its or the HSCIC’s duties under the DPA.
The Data Recipient shall implement and maintain security standards, facilities, controls and procedures appropriate to the nature of the Data held by it and the harm that would be caused by its loss or disclosure including a comprehensive and up-to-date data protection policy. The Data Recipient shall ensure that all its Personnel shall comply with the obligations upon them contained in the data protection policy.

The Data Recipient shall ensure:

4.1 that it has properly configured access rights for its Personnel including a well-defined joiners and leavers process to ensure access rights to the Data are properly managed;

4.2 that it has proper controls in place to make sure that complex alphanumeric passwords are required for access to the Data and that training is provided in relation to the need to keep such passwords secure;

4.3 it has in place procedures to identify wrongful use of Data, including the monitoring of wrongful access to Data;

4.4 suitable and effective authentication processes are established and used to protect Data;

4.5 Data is backed up on a regular basis and that any back up data which are subject to such vigorous security procedures as are necessary in order to protect data integrity, such security measures being commensurate to the nature of the data. The Data Recipient shall take particular care when transporting backup data and other personal information and shall ensure such backup data and other personal information is transported in a safe and secure manner;

4.6 Data transferred electronically is encrypted;

4.7 information stored on laptops or other portable media is encrypted and that the Data Recipient maintains an accurate, up to date asset register, including all such portable media used to process the Data;

4.8 that Personnel are not able to access the Data from home or via their own electronic device other than through a secure electronic network and that Data may not be stored in such devices;

4.9 that suitable physical security measures are established commensurate to the harm that could result from the unlawful disclosure of the Data. Such physical security measures shall be as identified in the Data Recipient's data protection policy;

4.10 without prejudice to the Data Recipient's obligations to the HSCIC in relation to the disposal of Data, all Data which is disposed of must be disposed of pursuant to the Data Recipient's policy for the disposal of Data identified in the data protection policy, including the disposal of assets containing personal data, a copy of which policy shall be provided, on request, to the HSCIC; and

4.11 that the Data Recipient establishes and maintains adequate data security compliance policies and audits its use of personal data in compliance with its data security policies on a regular basis and in any event annually.

The Data Recipient shall nominate in writing an individual to take responsibility and be accountable for compliance with the DPA, and shall provide to the HSCIC the name of that individual.
Part 2

1 It is Department of Health policy for all bodies that process NHS patient information to provide security assurance through annual completion and publication of an Information Governance (IG) Toolkit. The Department now wishes to seek this assurance from bodies that obtain NHS patient information in circumstances approved under section 251 of the National Health Service Act 2006 and supporting Regulations. A requirement within the Regulations is to ensure that appropriate technical and organisational measures are taken to prevent unauthorised processing of that information. Assurance over this aspect is now provided through satisfactory IG Toolkit submission including applications requiring sensitive data items approved by Data Access Advisory group (DAAG) and those covering access to Registration data approved by Office of National Statistics (ONS).

2 Security responsibilities of the Data Recipient:

2.1 The Data Recipient understands and accepts that it becomes a Data Controller for Personal Data received from the HSCIC. As such the Data Recipient is responsible for processing the Data in accordance with the DPA and maintaining good information governance standards and practices.

2.2 The Data Recipient understands and accepts that it shall be responsible for the security and protection of Non-Identifiable Data received from the HSCIC. The Data Recipient shall process such Non-Identifiable Data in accordance with all Applicable Laws.

3 To provide assurance that good information governance practices are being maintained, the Data Recipient must demonstrate, and will allow the HSCIC to audit, that it: (please complete one of the following three boxes)

Either

| Meets or exceeds the Information Governance Toolkit standards required for their organisation type |
| Organisation Code: | Score: |

Or

| Is Certified against international security standard ISO 27002 |
| Certification Details: |

Or

| Has other assurance in place |
| Details of Assurance: |

4 In cases where these assurance standards are not appropriate, the Data Recipient must ensure that it meets the requirements set out in paragraph 5 of this part 2 of Schedule 2, which the HSCIC reserves the right to audit.

5 The Data Recipient shall:
5.1 process Personal Data only for medical purposes, and only for purposes described in this Contract and the relevant DSA, and which are consistent with the purposes recorded in the Data Recipient’s data protection registration with the Information Commissioner’s Office;

5.2 process the minimum data necessary (e.g. using age range rather than age if sufficient);

5.3 deploy secure processes, procedures, practice and technology for storage and access, commensurate with the Personal Data being processed;

5.4 ensure the rights of individuals are met, such as satisfying subject access requests received, ensuring data accuracy and correcting errors, and handling objections and complaints;

5.5 destroy the Data once it is no longer required for the purpose for which it was collected and confirm destruction to the HSCIC;

5.6 ensures all Personnel with access to Personal Data provide a written undertaking that they understand and will act in accordance with the DPA, will not share passwords, and will protect the confidentiality of the Personal Data;

5.7 report immediately to the HSCIC any security incidents relating to the Data, and any instances of breach of any of the terms of this Contract; and

5.8 comply with any specific legislation in relation to the Data (such as the Statistics and Registration Services Act 2007).
SCHEDULE 3
List of relevant legislation and standards

- British (International) Standard ISO 27001
- The Caldicott Report 1997
- Information: To share or not to share? The Information Governance Review March 2013
- The Freedom of Information Act 2000
- Section 251 of the NHS Act 2006 (originally enacted under Section 60 of the Health and Social Care Act 2001)
- Confidentiality: NHS Code of Practice 2003
- Health and Social Care Act 2012
- The Computer Misuse Act 1990
- The Electronic Communications Act 2000
- The Copyright, Designs and Patents Act 1988
- [The Re-Use of Public Sector Information Regulations 2005]
- The Human Rights Act 1998
- The NHS Care Record Guarantee 2011 (Version 5)
- The Social Care Record Guarantee 2009
- Anonymisation Standard for Publishing Health and Social Care Data
SCHEDULE 4
Sub-licensing conditions

1 Where the HSCIC consents to the Data Recipient sub-licensing the Data to third parties, the HSCIC may impose conditions on such sub-licensing in the DSA. Conditions may include:
   1.1 the duration of the sub-licence;
   1.2 specification of the Data that may be sub-licensed;
   1.3 the identity of any third parties to whom the Data may be sub-licensed;
   1.4 the conditions on which the HSCIC may revoke the Data Recipient's right to sub-licence the Data; and
   1.5 any special conditions that must be met by the Data Recipient and/or the sub-licensee prior to any sharing of Data, which may include:
      1.5.1 any requirements to anonymise or pseudonymise the Data prior to onward sharing;
      1.5.2 a requirement for the Data Recipient to comply with any instructions issued by the HSCIC in respect of the Data;
      1.5.3 any specific exclusions to the scope of the sub-licence; and
      1.5.4 any audit rights that the HSCIC may require to ensure compliance with these sub-licence conditions.

2 Breach of any sub-licensing conditions by the Data Recipient shall entitle the HSCIC to terminate the relevant DSA and/or this Contract.