

Data Sharing Memorandum of Understanding

CONTENTS

CLAUSE

1.	<i>Interpretation</i>	1
2.	<i>Agreed Purpose</i>	3
3.	<i>Compliance with national data protection laws</i>	3
4.	<i>Shared Personal Data</i>	3
5.	<i>Lawful, fair and transparent processing</i>	4
6.	<i>Data quality</i>	
7.	<i>NHS Conditions</i>	
8.	<i>Data subjects' rights</i>	4
9.	<i>Data retention and deletion</i>	5
10.	<i>Transfers</i>	5
11.	<i>Security and training</i>	6
12.	<i>Personal data breaches and reporting procedures</i>	6
13.	<i>Resolution of disputes with data subjects or the Supervisory Authority</i>	6
14.	<i>Parties' Responsibilities</i>	7
15.	<i>Allocation of cost</i>	7
16.	<i>Third party rights</i>	8
17.	<i>Variation</i>	8
18.	<i>Waiver</i>	88
19.	<i>Changes to the applicable law</i>	8
20.	<i>Entire agreement</i>	9
21.	<i>Further assurance</i>	9
22.	<i>Force majeure</i>	9
23.	<i>No Legal Effect</i>	
24.	<i>Notice</i>	9
25.	<i>Governing law and Jurisdiction</i>	10

This Memorandum of Understanding is dated the date on which the Lead Local Authority downloads the Shared Personal Data under clause 1.12.

PARTIES

- (1) The Government Digital Service, acting as part of the Cabinet Office, of The Whitechapel Building, 10 Whitechapel High Street, London, E1 8QS (**the Cabinet Office**); and
- (2) **The Lead Local Authority**

BACKGROUND

- (A) The Cabinet Office acting through the Government Digital Service (**GDS**), has been commissioned by the Prime Minister to develop an online and telephone service for extremely vulnerable patients. Information about the service is here: <https://www.gov.uk/coronavirus-extremely-vulnerable>. The service will provide those individuals with a way to seek help and support whilst they are self-isolating to protect themselves from the COVID-19 virus, including by providing a means to ask for social care support and essential food and supplies (**the Service**). The Cabinet Office is the Controller (as defined in the Data Protection Legislation) for the personal data processed as part of the Service.
- (B) The Cabinet Office has created a list of Vulnerable Persons within each Local Authority area derived from the NHS List (**the Shared Personal Data**). The Shared Personal Data contains Personal Data and Special Category Personal Data relating to the individuals named within it.
- (C) The Cabinet Office will provide the Lead Local Authority with access to the Shared Personal Data. The Lead Local Authority will receive the Shared Personal Data on behalf of itself and each Local Authority (**Relying Local Authorities**) within the Lead Local Authority's Hub. The Lead Local Authority will transmit the Shared Personal Data relating to individuals resident within a Local Authority area to the relevant Local Authority within the Hub.
- (D) The Local Authorities will use the Shared Personal Data to cross check which of those patients are existing local authority social care service users or are otherwise known to the local authority to be vulnerable, to enable the Local Authorities contact those individuals to offer them help with the provision of essential supplies and support to meet their care and welfare needs
- (E) This MoU facilitates the provision of access to the personal data securely held by GDS to the Lead Local Authority acting on behalf of the Relying Local Authorities, and documents the roles and responsibilities of each Party (as defined below).

AGREED TERMS

1. Interpretation

The following definitions and rules of interpretation apply in this Cabinet Office.

1.1 Definitions:

- 1 **Agreed Purpose:** has the meaning given to it in clause 2 of this Agreement.
- 2 **Business Day:** a day other than a Saturday, Sunday or public holiday in England when banks in London are open for business.
- 3 **Commencement Date:** 1st April 2020.
- 4 **Deletion Procedure:** has the meaning given to it in clause 8.3 and Schedule 8 to this Agreement.
- 5 **Data Sharing Code:** the Information Commissioner's Data Sharing Code of Practice of May 2011, as updated or amended from time to time.
- 6 **Data Protection Legislation:** all applicable data protection and privacy legislation in force from time to time in the UK including the General Data Protection Regulation ((EU) 2016/679) (**GDPR**); the Data Protection Act 2018; the Privacy and Electronic Communications Directive 2002/58/EC (as updated by Directive 2009/136/EC) and the Privacy and Electronic Communications Regulations 2003 (SI 2003 No. 2426) as amended; any other European Union legislation relating to personal data and all other legislation and regulatory requirements in force from time to time which apply to a party relating to the use of Personal Data (including, without limitation, the privacy of electronic communications).
- 7 **GDS:** has the meaning given in Recital A.
- 8 **Hub:** means the hub of Local Authorities on whose behalf the Lead Local Authority is acting.
- 9 **Local Authority:** means the Lead Local Authority and any of the Relying Local Authorities.
- 10 **NHS List:** means a list produced by the NHS, also known as the "*Shielded Patients List*" which contains the name, address, date of birth (**DOB**), phone number and NHS number for those individuals who have been identified by clinicians as being extremely vulnerable in relation to the COVID-19 virus as a result of their pre-existing medical conditions.
- 11 **Personal Data Breach:** a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the Shared Personal Data.
- 12 **Relying Local Authorities:** has the meaning given in Recital B.
- 13 **Shared Personal Data:** has the meaning given in Recital B.
- 14 **Subject Access Request:** the exercise by a data subject of his or her rights under Article 15 of the GDPR and the DPA 2018.
- 15 **Supervisory Authority:** the relevant supervisory authority in the territories where the parties to this Agreement are established.
- 16 **Term:** means the period commencing on Commencement Date and ending on 30th September 2020 (**End Date**)
- 17 **Vulnerable Persons:** individuals who HM Government, in conjunction with the NHS has identified and verified as being clinically extremely vulnerable to COVID-19 as a result of the pre-existing medical condition
- 18 **Controller, Processor, Data Subject and Personal Data, Special Categories of Personal Data, Processing** and "appropriate technical and organisational measures" shall have the meanings given to them in the Data Protection Legislation.
- 1.2 Clause, schedule and paragraph headings shall not affect the interpretation of this Agreement.
- 1.3 The schedules form part of this Agreement and shall have effect as if set out in full in the body of this Agreement. Any reference to this Agreement includes the schedules.

- 1.4 Unless the context otherwise requires, words in the singular shall include the plural and in the plural shall include the singular.
- 1.5 A reference to a company shall include any company, corporation or other body corporate, wherever and however incorporated or established.
- 1.6 A reference to a statute or statutory provision shall include all subordinate legislation made from time to time under that statute or statutory provision.
- 1.7 References to clauses and Schedules are to the clauses and Schedules of this Cabinet Office and references to paragraphs are to paragraphs of the relevant Schedule.
- 1.8 Any words following the terms **including**, **include**, **in particular** or **for example** or any similar phrase shall be construed as illustrative and shall not limit the generality of the related general words.
- 1.9 In the case of any ambiguity between any provision contained in the body of this MoU and any provision contained in the Schedules or appendices, the provision in the body of this MoU shall take precedence.
- 1.10 A reference to **writing** or **written** includes fax and email.
- 1.11 Unless the context otherwise requires the reference to one gender shall include a reference to the other genders.

Commencement

- 1.12 By emailing this MoU to the Lead Local Authority the Cabinet Office has offered to enter into an MoU on the terms set out herein. By downloading the Shared Personal Data the Lead Local Authority is deemed to have accepted the terms of this MoU.

2. Agreed Purpose

- 2.1 The Parties to this MoU are each Independent Controllers in relation to the Shared Personal Data.
- 2.2 The Lead Local Authority will be receiving the Shared Personal Data on behalf of itself and each of the Relying Local Authorities. Before sharing any of the Shared Personal Data with any of the Relying Local Authorities, the Lead Local Authority shall ensure that it puts in place appropriate data sharing arrangements with each of the Relying Local Authorities.
- 2.3 This MoU sets out the framework for the sharing of **Personal Data** when one **Controller** discloses personal data to another **Controller**. It defines the principles and procedures that the parties shall adhere to and the responsibilities the parties owe to each other.
- 2.4 The parties agree to only process Shared Personal Data, (as described in clauses 4.1 and 4.2) for the purpose of enabling Local Authorities to cross check which of those patients are existing local authority social care service users or are otherwise known to the local authority to be vulnerable to enable local authorities to prioritise contacting those individuals to offer them help, social care and support (**Agreed Purpose**).
- 2.5 The parties shall:
 - (a) ensure that the Shared Personal Data is kept confidential at all times; and

- (b) shall not process Shared Personal Data in a way that is incompatible with the purposes described in this clause.

2.6 Each party shall appoint a single point of contact (**SPoC**) who will work together to reach an agreement with regards to any issues arising from the data sharing and to actively improve the effectiveness of the data sharing initiative. The points of contact for each of the parties are:

- (a) gds-privacy-office@digital.cabinet-office.gov.uk
- (b) The Lead Local Authority shall provide the Cabinet Office with details of their SPoC within 3 working days of the Commencement Date.

3. Compliance with national data protection laws

3.1 Each Party must ensure compliance with applicable Data Protection Legislation at all times during the Term of this MoU.

3.2 Each party has such valid registrations and paid such fees as are required by its national Supervisory Authority which, by the time that the data sharing is expected to commence, covers the intended data sharing pursuant to this Agreement, unless an exemption applies.

4. Shared Personal Data

4.1 The Shared Personal Data contains the following types of Personal Data which will be provided by the Cabinet Office to the Lead Local Authority during the Term of this MoU:

- (a) Names;
- (b) Dates of Birth;
- (c) NHS number
- (d) Addresses and post codes;
- (e) Mobile and landline telephone numbers; and
- (f) Email addresses

of Vulnerable Persons .

4.2 The following types of special categories of Personal Data will be shared between the Parties during the Term of this MoU:

- (a) The inclusion of Vulnerable Persons in the Shared Personal Data will indicate they have a pre-existing medical condition which makes them extremely vulnerable to COVID-19 but no specific information on medical conditions will be shared;

4.3 The Shared Personal Data must not be irrelevant or excessive with regard to the Agreed Purposes.

5. Lawful, fair and transparent processing

5.1 Each party shall ensure that it processes the Shared Personal Data fairly and lawfully in accordance with clause 5.2 during the Term of this MoU.

5.2 The Cabinet Office relies on the following lawful bases for processing the Shared Personal Data:

- (a) the processing is necessary for the performance of a task carried out in the public interest under Article 6(1)(e) of GDPR;
- (b) the processing is necessary for reasons of substantial public interest performance of a task carried out in the public interest under Article 9(2)(g) of GDPR; and
- (c) the processing is necessary under paragraph 6 of Schedule 1 of the Data Protection Act 2018.

5.3 The Lead Local Authority relies on the following lawful bases for processing the Shared Personal Data:

- (a) the processing is necessary for the performance of a task carried out in the public interest under Article 6(1)(e) of GDPR;
- (b) the processing is necessary for reasons of substantial public interest performance of a task carried out in the public interest under Article 9(2)(g) of GDPR; and
- (c) the processing is necessary under paragraph 6 of Schedule 1 of the Data Protection Act 2018.

5.4 The Lead Local Authority shall undertake to inform the Data Subjects, in accordance with the Data Protection Legislation, of the purposes for which it will process their personal data, the legal basis for such purposes and such other information as is required by Article 14 of the GDPR including:

- (a) giving full information to any data subject whose personal data may be processed under this arrangement of the nature such processing.
- (b) the fact that Shared Personal Data will be transferred to the Relying Local Authorities and sufficient information about such transfer and the purpose of such transfer to enable the data subject to understand the purpose and risks of such transfer.

6. Data quality

6.1 The Cabinet Office makes no warranty as to the accuracy or completeness of the Shared Personal Data.

6.2 Shared Personal Data must be limited to the Personal Data described in clause 4.1 and clause 4.2, and Schedule 4 of this Agreement.

7. NHS Conditions

7.1 Without limiting any other term of this MoU, the Cabinet Office is providing the Shared Personal Data in accordance with the following conditions:

- (a) the Shared Personal Data contains confidential patient information derived from the NHS List. This information is provided in confidence and must be maintained and handled by the Local Authorities as confidential information to which a common law duty of confidence applies.
- (b) that the NHS List was produced on 20th March 2020 based on information held in NHS central records. Consequently, the Shared Personal Data may contain information about individuals who are now deceased.
- (c) that from 28th March, an outbound central call centre operated by the Department

- (d) individuals who are on the NHS List but who have not yet contacted the Service, to offer them information about the Service and support.
- (e) That the Shared Personal Data are to be used for the sole purpose in clause 2.4 and are not to be shared outside of the Relying Local Authorities.

7.2 The Lead Local Authority acknowledges and agrees that the Shared Personal Data is derived from the NHS List and consequently Local Authorities have a statutory requirement to process any such confidential patient information for purposes set out in Regulation 3(1) of the Health Service Control of Patient Information Regulations 2002 (COPI) under the notice dated 20th March 2020 issued to them by the Secretary of State for Health and Social Care under Regulation 3(4) of COPI (the **COPI Notice**) until 20th September 2020.

8. Data subjects' rights

8.1 The parties each agree to provide such assistance as is reasonably required to enable the other party to comply with requests from Data Subjects to exercise their rights under the Data Protection Legislation within the time limits imposed by the Data Protection Legislation.

8.2 The SPoC for each party is responsible for maintaining a record of individual requests for information, the decisions made and any information that was exchanged. Records must include copies of the request for information, details of the data accessed and shared and where relevant, notes of any meeting, correspondence or phone calls relating to the request. The SPoC for each party are detailed in clause 2.4.

9. Data retention and deletion

9.1 The Lead Local Authority shall not retain or process Shared Personal Data for longer than is necessary to carry out the Agreed Purposes.

9.2 Notwithstanding clause 8.1, parties shall continue to retain Shared Personal Data in accordance with any statutory or professional retention periods applicable in their respective countries and / or industry.

9.3 The Lead Local Authority shall ensure that any Shared Personal Data are returned to the Cabinet Office or destroyed in the following circumstances:

- (a) on termination of the Agreement;
- (b) on expiry of the Term of the Agreement; or
- (c) once processing of the Shared Personal Data is no longer necessary for the purposes it was originally shared for, as set out in clause 2.3.

9.4 Following the deletion of Shared Personal Data in accordance with clause 8.3, the Lead Local Authority shall notify the Cabinet Office that the Shared Personal Data in question has been deleted.

10. Transfers

10.1 For the purposes of this clause, transfers of personal data shall mean any sharing of personal data by the Lead Local Authority with a third party, and shall include, but is not limited to, the following:

- (a) subcontracting the processing of Shared Personal Data;

(b) granting a third party controller access to the Shared Personal Data.

10.2 The Lead Local Authority shall not transfer the Shared Personal Data to a third party other than the Relying Local Authorities.

10.3 The Lead Local Authority may not transfer Shared Personal Data to a third party located outside the EEA.

11. Security and training

11.1 The Cabinet Office shall only provide the Shared Personal Data to the Lead Local Authority by using secure methods as agreed and set out in Schedule 1.

11.2 The parties undertake to have in place throughout the Term appropriate technical and organisational security measures to:

(a) prevent:

- (i) unauthorised or unlawful processing of the Shared Personal Data; and
- (ii) the accidental loss or destruction of, or damage to, the Shared Personal Data

(b) ensure a level of security appropriate to:

- (i) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage; and
- (ii) the nature of the Shared Personal Data to be protected.

11.3 It is the responsibility of each party to ensure that its staff members are appropriately trained to handle and process the Shared Personal Data in accordance with appropriate technical and organisational security measures together with any other applicable national data protection laws and guidance and have entered into confidentiality agreements relating to the processing of personal data.

12. Personal data breaches and reporting procedures

12.1 The parties shall each comply with its obligation to report a Personal Data Breach to the appropriate Supervisory Authority and (where applicable) data subjects under Article 33 of the GDPR and shall each inform the other party of any Personal Data Breach irrespective of whether there is a requirement to notify any Supervisory Authority or data subject(s).

12.2 The parties agree to provide reasonable assistance as is necessary to each other to facilitate the handling of any Personal Data Breach in an expeditious and compliant manner.

13. Resolution of disputes with data subjects or the Supervisory Authority

13.1 In the event of a dispute or claim brought by a data subject or the Supervisory Authority concerning the processing of Shared Personal Data against either or both parties, the parties will inform each other about any such disputes or claims, and will cooperate with a view to settling them amicably in a timely fashion.

13.2 The parties agree to respond to any generally available non-binding mediation procedure initiated by a data subject or by the Supervisory Authority. If they do participate in the proceedings, the parties may elect to do so remotely (such as by telephone or other electronic means). The parties

also agree to consider participating in any other arbitration, mediation or other dispute resolution proceedings developed for data protection disputes.

13.3 Each party shall abide by a decision of a competent court of the Cabinet Office's country of establishment or of the Supervisory Authority.

14. Parties' Responsibilities

14.1 Each party will:

- (a) Process the Shared Personal Data in compliance with all applicable laws, enactments, regulations, orders, standards and other similar instruments that apply to its personal data processing operations.
- (b) Respond within a reasonable time and as far as reasonably possible to enquiries from the relevant Supervisory Authority in relation to the Shared Personal Data.
- (c) Respond to Subject Access Requests in accordance with the Data Protection Legislation.
- (d) Where applicable, maintain registration with all relevant Supervisory Authorities to process all Shared Personal Data for the Agreed Purpose; and
- (e) Take all appropriate steps to ensure compliance with the security measures set out in 10 above.

14.2 The Lead Local Authority warrants and undertakes that it will not disclose or transfer the Shared Personal Data to a third party controller located outside the EEA unless it complies with the obligations set out in clause 9.3 above.

14.3 Except as expressly stated in this MoU, all warranties, conditions and terms, whether express or implied by statute, common law or otherwise are hereby excluded to the extent permitted by law.

15. Allocation of cost

Each party shall perform its obligations under this MoU at its own cost.

16. Third party rights

16.1 No one other than a party to this MoU, their successors and permitted assignees,] shall have any right to enforce any of its terms.

17. Variation

No variation of this MoU shall be effective unless it is in writing and signed by the parties (or their authorised representatives).

18. Waiver

No failure or delay by a party to exercise any right or remedy provided under this MoU or by law shall constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict the further exercise of that or any other right or remedy. No single or partial exercise of such right or remedy shall prevent or restrict the further exercise of that or any other right or remedy.

19. Changes to the applicable law

If during the Term the Data Protection Legislation change in a way that the MoU is no longer adequate for the purpose of governing lawful data sharing exercises, the Parties agree that the SPoCs will negotiate in good faith to review the MoU in the light of the new legislation.

20. Entire agreement

20.1 This MoU constitutes the entire agreement between the parties and supersedes and extinguishes all previous agreements, promises, assurances, warranties, representations and understandings between them, whether written or oral, relating to its subject matter.

20.2 Each party acknowledges that in entering into this MoU it does not rely on, and shall have no remedies in respect of any statement, representation, assurance or warranty (whether made innocently or negligently) that is not set out in this MoU.

20.3 Each party agrees that it shall have no claim for innocent or negligent misrepresentation or negligent misrepresentation based on any statement in this MoU.

21. Further assurance

At its own expense, each party shall, and shall use all reasonable endeavours to procure that any necessary third party shall, promptly execute and deliver such documents and perform such acts as may be required for the purpose of giving full effect to this MoU.

22. Force majeure

Neither party shall be in breach of this MoU nor liable for delay in performing, or failure to perform, any of its obligations under this MoU if such delay or failure result from events, circumstances or causes beyond its reasonable control. In such circumstances [the time for performance shall be extended by a period equivalent to the period during which performance of the obligation has been delayed or failed to be performed. If the period of delay or non-performance continues for 3 months, the party not affected may terminate this MoU by giving 30 days' written notice to the affected party.

23. No Legal Effect

The parties intend to comply with their respective legal obligations under this MoU. However, this MoU does not give rise to any enforceable legal obligations between the parties whether in the law of contract or otherwise.

24. Notice

24.1 Any notice or communication given to a party under or in connection with this MoU shall be in writing, addressed to the SPoCs and shall be:

- (a) delivered by hand or by pre-paid first-class post or other next working day delivery service at its registered office (if a company) or its principal place of business (in any other case); or
- (b) sent by email to the SPoC.

24.2 Any notice or communication shall be deemed to have been received:

- (a) if delivered by hand, on signature of a delivery receipt or at the time the notice is left at the proper address; and
- (b) if sent by pre-paid first-class post or other next working day delivery service, at 9.00 am on the second Business Day after posting or at the time recorded by the delivery service; and
- (c) if sent by email, at the time of transmission, or if this time falls outside business hours in the place of receipt, when business hours resume. In this 26.2(c), business hours means 9:00 am to 5:00 pm Monday to Friday on a day that is not a public holiday in the place of receipt.

24.3 This clause does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution

25. Governing law and Jurisdiction

This MoU shall be governed by and construed in accordance with the law of England and Wales. and each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim (including non-contractual disputes or claims) arising in respect of this MoU.

- END OF MOU Terms -

Schedule 1

Security

The Cabinet Office will provide the Shared Personal Data via a secure and encrypted two factor authentication mechanism (to be agreed between Mark Reynolds of NHS Digital and Stephen Harker of GDS), to the Lead Local Authority.