**DATA SHARING AGREEMENT**

**THIS AGREEMENT** is made on \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **BETWEEN**:

1. **THE CHANCELLOR MASTERS AND SCHOLARS OF THE UNIVERSITY OF OXFORD**, whose administrative office is at University Offices, Wellington Square, Oxford, OX1 2JD, United Kingdom (“**Oxford**”); and
2. **[INSERT NAME]**, [insert address] (the “**Data User**”),

each a “**Party**” and collectively the “**Parties**”.

**BACKGROUND**

1. Oxford and Peking University are jointly conducting a project known as the China Kadoorie Biobank.
2. The Data User wishes to have access to data from the China Kadoorie Biobank and Oxford is willing to provide the data to the Data User subject to the following terms and conditions.

**NOW IT IS AGREED as follows**:

# DEFINITIONS AND INTERPRETATION

## In this Agreement the following terms have the following meanings:

|  |  |
| --- | --- |
| **Access Charge** | the sum payable under this Agreement by the Data User to Oxford for providing access to the Data, as set out in Schedule 3 (Access Charges). |
| **Approved Application** | the application approved by Oxford, as set out in Schedule 1 (Approved Application). |
| **Approved Research** | the research activities approved by Oxford, as set out in the Approved Application. |
| **Arising Intellectual Property** | all Intellectual Property that is conceived, generated, or developed in the course of carrying out the Approved Research, including any Intellectual Property in the Results. |
| **Background Intellectual Property** | all Intellectual Property (except any Arising Intellectual Property) that is owned by, or licensed to, a Party:existing prior to the Effective Date; and/ordeveloped or acquired independently of this Agreement. |
| **Data** | the data to be provided by Oxford to the Data user, as set out in Schedule 2 and any Update. |
| **Effective Date** | the date of this Agreement as written above. |
| **Intellectual Property** | patents, petty patents, utility models, any extensions of the exclusivity granted in connection with the foregoing (including supplementary protection certificates), registered designs, plant variety rights, applications for any of the foregoing (including, continuations, continuations-in-part and divisional applications), the right to claim priority from, the right to apply for and be granted any of the foregoing, rights in inventions, copyrights, design rights, semiconductor topography rights, database rights, publication rights, performance rights, rights in know-how, trade secrets and confidential information and all other forms of intellectual property right which may exist now or in the future anywhere in the world. |
| **Peking** | Peking University, whose administrative office is at NO.5 Yiheyuan Road, Haidian District, Beijing 100871, P. R. China |
| **Personnel** | officers, employees, workers, contract staff, consultants, agents, representatives, advisers and students. |
| **Publish** and **Publication** | the publication of an abstract, article or paper or the presentation of information at a conference or external seminar. |
| **Results** | all results, discoveries, inventions (whether patentable or not), data (including raw data), methods, techniques, protocols, findings and any other information created or generated in the course of carrying out the Approved Research. |
| **Study** | the China Kadoorie Biobank Study, a blood-based prospective study of the main genetic and non-genetic causes of common chronic diseases in Chinese population. |
| **Term** | the period commencing on the Effective Date and ending on the earlier of:[insert date] **OR** [the conclusion of the Approved Research] or any later date agreed in writing by the duly authorised representatives of both Parties; orthe date of which this Agreement is terminated in accordance with the provisions of this Agreement. |
| **Update** | any update to the Data issued by Oxford to the Data User from time to time. |

## In this Agreement:

### any phrase introduced by the terms “including”, “include” and “in particular” or any similar expression shall be construed as illustrative only and shall not limit the sense of the words preceding these terms;

### the headings are for convenience only and shall not affect the interpretation of this Agreement;

### the meaning given to defined terms in this Agreement shall also apply to their grammatical variants provided that the initial letter is capitalised; and

### a reference to a statute or statutory provision is a reference to that statute or statutory provision as amended, extended, consolidated or re-enacted from time to time and shall include all subordinate legislation made from time to time under that statute or statutory provision.

# LICENCE

## Subject to payment of the Access Charges, Oxford grants to the Data User a non-exclusive, non-transferable, non-sub-licensable, royalty-free licence for the Term to use the Data solely for the purpose of carrying out the Approved Research.

# LICENCE CONDITIONS

## The Data User shall pay to Oxford the Access Charges.

## The Data User shall:

### comply with all applicable laws in respect of the Data;

### only make the Data available to its Personnel who require access in order to conduct the Approved Research;

### ensure that no activities are carried out with the Data that are not strictly necessary for the conduct of the Approved Research; and

### ensure that it has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of the Data and against accidental loss or destruction of, or damage to, the Data.

## The Data User shall not:

### make the Data available to a third party (through a transfer, disclosure or in any way whatsoever) without prior written consent of Oxford;

### link the Data with any other data unless clearly described in the Approved Application; or

### attempt to identify any identifiable living or deceased individual from the Data.

## The Data User shall promptly submit annual reports (starting on the first anniversary of the Effective Date) and any other information reasonably requested by Oxford to evidence the work undertaken by the Data User in connection with the Approved Research.

## Unless otherwise agreed by the Parties in writing, Oxford and Peking shall be entitled to publish on the Study website a summary of the Approved Research and summary details of the Data User.

## The Parties shall comply with the provisions of Schedule 4 (Data Protection).

# INTELLECTUAL PROPERTY

## Nothing in this Agreement shall affect the ownership of either Party's Background Intellectual Property. No licence to use any Intellectual Property is granted or implied by this Agreement except for the rights expressly granted in this Agreement.

## The Results and Arising Intellectual Property shall be owned by the Data User.

## The Data User grants to Oxford a non-exclusive, non-transferable, non-sub-licensable (except in accordance with Clause 4.4), irrevocable, royalty-free licence to use its Arising Intellectual Property for teaching and research (including research funded by any third parties, provided that those parties gain or claim no rights to such Arising Intellectual Property).

## Oxford shall be permitted to sub-license its rights to the Arising Intellectual Property to Peking and the government of the People’s Republic of China.

# PUBLICATION

## Where the Data User wishes to submit the Results for Publication, the Data User will submit the proposed Publication to Oxford at least thirty (30) days before the date of the proposed submission for Publication or, in the case or presentations, posters and abstracts, at least ten (10) days before the proposed date of presentation or submission for Publication. Oxford agrees not to disclose any Results contained in such advance copy to any third party until published by the Data User.

## The Data User shall comply with recognised standards concerning publication and authorship, including the *Uniform Requirements for Manuscripts Submitted to Biomedical Journals* issued by the International Committee of Medical Journal Editors.

## The Data User shall include the following acknowledgement in any publication of the Results:

## “This research has been conducted using the China Kadoorie Biobank (CKB) Resource (www.ckbiobank.org). Publication of results does not require or imply approval by the membership of the CKB Collaborative Group. The CKB has received funding from the British Heart Foundation, Cancer Research UK, Chinese Ministry of Science and Technology, Chinese National Natural Science Foundation, the Kadoorie Charitable Foundation in Hong Kong, Medical Research Council – UK Research and Innovation and the Wellcome Trust.”

## This acknowledgement should, when possible, be linked to reference search tools (such as PubMed and MEDLINE).

# LIABILITY

## Except to the extent prohibited by law, the Data User assumes all direct liability for damages which may arise from its use of the Data. Oxford will not be liable to the Data User for any use made of the Data, including any loss, claim or demand made by the Data User or made against the Data User by a third party, due to or arising from the use of the Data by the Data User, except to the extent permitted by law when caused by the gross negligence or wilful misconduct of Oxford.

## Oxford provides the Data ‘as is’ and makes no representation and gives no warranty of any kind, either express or implied, including warranties of accuracy or fitness for a particular purpose, or that the use of the Data will not infringe any patent, copyright, trademark or other proprietary rights. The Data cannot be guaranteed to be free from errors, omissions or inaccuracies, accordingly Oxford will not be liable to the Data User for any loss, damage, claim or liability arising from any reliance placed on the Data by the Data User.

## Neither Party accepts any liability or responsibility for any use which may be made by the other Party of any of the Results or Arising Intellectual Property, nor for any reliance which may be placed by that other Party on any of Results or Arising Intellectual Property, nor for any advice or information given in connection with the Approved Research or any of the Results or Arising Intellectual Property.

## The liability of each Party to the other for any breach of this Agreement, any negligence, or arising in any other way out of the subject matter of this Agreement, the Approved Research, the Results and the Arising Intellectual Property, shall not extend to:

### any indirect damages or losses; or

### any loss of profits, loss of revenue, loss of contracts or loss of opportunity, whether direct or indirect,

## even if the Party bringing the claim has advised the other of the possibility of those losses, or if they were within the other Party's contemplation.

## Nothing in this Agreement shall exclude or limit a Party’s liability in respect of any liability that cannot be excluded or limited pursuant to applicable law including the following liabilities, to the extent that they cannot be excluded or limited by law:

### death or personal injury caused by negligence; and

### bribery, fraud or fraudulent misrepresentation.

# TERM AND TERMINATION

## This Agreement shall commence on the Effective Date and shall continue, unless terminated earlier in accordance with this Clause 7 (Term and Termination), until expiry at the end of the Term.

## Each Party shall have the right to terminate this Agreement with immediate effect and without affecting any other right or remedy available to that Party by giving notice to the other Party if:

### the other Party commits a material breach of any term of this Agreement which breach is irremediable or (if such breach is remediable) fails to remedy that breach within a period of thirty (30) days after being notified to do so; or

### the other Party becomes insolvent; an order is made or a resolution is passed for the winding up of the other Party (other than voluntarily for the purpose of solvent amalgamation or reconstruction); an administrator, administrative receiver or receiver is appointed in respect of the whole or any part of the other Party's assets or business; the other Party makes any composition with the other Party’s creditors; or the other Party takes or suffers any similar or analogous action in consequence of debt.

## Promptly following termination or expiry of this Agreement or at any other time upon Oxford’s request, the Data User shall either return or destroy (as instructed by Oxford at the relevant time) the Data and shall continue to abide by the obligations and restrictions set out in this Agreement. Destruction (if applicable) shall be confirmed in writing to Oxford.

## Any provision of this Agreement which either expressly or by implication is intended to come into, or continue in, effect on or after the termination or expiry of this Agreement shall continue in effect.

# GENERAL

## *Force majeure*. Neither Party shall be in breach of this Agreement nor liable for delay in performing, or failure to perform, any of its obligations under this Agreement if such delay or failure results from events, circumstances or causes beyond its reasonable control. In such circumstances, the affected Party shall be entitled to a reasonable extension of the time for performing such obligations. If the period of delay or non-performance continues for three (3) months, the Party not affected may terminate this Agreement by giving thirty (30) days' notice to the affected Party.

## *Assignment*. Neither Party shall assign, delegate, sub-contract or otherwise transfer or deal in any or all of its rights and obligations under this Agreement without the prior written consent of the other Party.

## *No use of names or logos*. Neither Party shall use the name or any logo of the other Party in any press release or product advertisement, or for any other promotional purpose, without the other Party's prior written consent.

## *Entire agreement*. This Agreement constitutes the entire agreement and understanding of the Parties relating to the subject matter of this Agreement and supersedes any prior agreement or understanding between the Parties relating to the subject matter of this Agreement. The Parties acknowledge that in entering into this Agreement they do not rely on any statement, representation (including any negligent misrepresentation but excluding any fraudulent misrepresentation), warranty, course of dealing, custom or understanding. The Parties irrevocably and unconditionally waive any rights and/or remedies they may have to the fullest extent permitted by law (including the right to claim damages and/or to rescind this Agreement) in respect of any misrepresentation (including any negligent misrepresentation but excluding any fraudulent misrepresentation).

## *Variation*. No change shall be made to this Agreement except in writing signed by the duly authorised representatives of both Parties.

## *Waiver*. No failure or delay by a Party to exercise any right or remedy provided under this Agreement or by law shall constitute a waiver of that or any other right or remedy, nor shall such failure or delay 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.

## *Severance*. If any provision or part-provision of this Agreement is or becomes invalid, illegal or unenforceable, such provision or part-provision shall, to the minimum extent required, be deemed deleted from this Agreement without affecting the validity and enforceability of the rest of this Agreement. In the event of any such deletion, the Parties shall negotiate in good faith in order to agree the terms of an alternative provision that, to the greatest extent possible, achieves the intended commercial result of the deleted provision.

## *Language*. This Agreement is drafted in the English language. If this Agreement is translated into any other language, the English language version shall prevail.

## *No partnership or agency*. Nothing in this Agreement creates, implies or evidences any partnership or joint venture between the Parties, or the relationship between them of principal and agent. Neither Party has any authority to make any representation or commitment, or to incur any liability, on behalf of the other Party.

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

## *Notices*. Any notice given to a Party under or in connection with this Agreement shall be in writing in English and shall be sent by email and either: (a) pre-paid first-class post if the sender and recipient are both based in the United Kingdom; or (b) courier in all other instances. Notices shall be addressed as follows:

### Notices to Oxford: The Executive Director, Research Services, University Offices, Wellington Square, Oxford OX1 2JD; email: [research.services@admin.ox.ac.uk](mailto:research.services@admin.ox.ac.uk) (using in each case the following reference: R48829).

### Notices to the Data User: [insert job title, address and email address] (using the reference: [insert reference]).

## Any written notice sent by a Party that is actually received by the other Party shall be deemed to have been properly given and received by that Party irrespective of whether or not the delivery requirements of this Clause 8.11 have been complied with.

## *Dispute resolution*. If the Parties are unable to reach agreement on any issue concerning this Agreement or the subject matter of this Agreement within fourteen (14) days after one Party has notified the other Party of that issue, they shall refer the matter to the Executive Director of Research Services in the case of Oxford, and to [insert officer] in the case of the Data User in an attempt to resolve the issue within fourteen (14) days after the referral. A Party may commence proceedings in accordance with Clause 8.14 (Jurisdiction) if the matter has not been resolved within that fourteen (14) day period, and a Party may apply to the court for an injunction, whether or not any issue has been referred for resolution under this Clause 8.12 (Dispute Resolution).

## *Governing law*. This Agreement and any dispute or claim arising out of or in connection with the Approved Research, this Agreement, or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with English law.

## *Jurisdiction*. The Parties submit irrevocably to the exclusive jurisdiction of the English Courts in relation to any dispute or claim arising out of or in connection with this Agreement or this Agreement’s subject matter or formation (including non-contractual disputes or claims), except that either Party may seek an interim injunction or equivalent remedy in any court of competent jurisdiction to protect its Intellectual Property or Confidential Information.

## *Counterparts*. This Agreement may be executed in any number of counterparts, each of which when executed shall constitute a duplicate original, but all the counterparts shall together constitute the one agreement. No counterpart shall be effective until each Party has executed and delivered to the other Party at least one counterpart.

**IN WITNESS of this Agreement**, the Parties have executed this Agreement through their duly authorised representatives.

|  |  |  |
| --- | --- | --- |
| **SIGNED** for and on behalf of **THE CHANCELLOR MASTERS AND SCHOLARS OF THE UNIVERSITY OF OXFORD** | )  )  )  ) |  |
| Name: |  | |
| Title: |  | |
| Date: |  | |

|  |  |  |
| --- | --- | --- |
| **SIGNED** for and on behalf of **[DATA USER]** | )  )  )  ) |  |
| Name: |  | |
| Title: |  | |
| Date: |  | |

# Schedule 1 – Approved Application

[Insert the Approved Application].

**Schedule 2 –Data**

[Insert a description of the Data to be provided to the Data User].

**Schedule 3 – Access Charges**

[Insert any access charges].

The Data User shall pay the access charges, subject to first receiving an invoice issued by Oxford. Oxford shall include on its invoices any purchase order or other reference number notified in writing by the Data User to Oxford.

Invoices should be submitted to: [insert email address].

**Schedule 4 – Data Protection**

**DEFINITIONS**

**Controller**, **processor**, **data subject**, **personal data**, and **processing**: as set out in the Data Protection Legislation in force at the time.

**Data Protection Legislation**: any law, statute, declaration, decree, directive, legislative enactment, order, ordinance, regulation, rule or other binding restriction (as amended, consolidated or re-enacted from time to time) which relates to the protection of individuals with regards to the Processing of Personal Data to which a Party is subject, including the Data Protection Act 2018 and retained EU law version of the General Data Protection Regulation ((EU) (2016/679)) (“**GDPR**”).

**Personal Data Breach**: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

**Personal Data**: any personal data (as defined in the Data Protection Legislation) Processed by either Party in connection with this Agreement.

**Approved Research Personal Data:** any personal data shared between the Parties for the purposes of the Approved Research or generated by the Approved Research.

**Relevant Transfer**: a transfer of personal data from Oxford to the Data User where the Data User will receive the data in a jurisdiction that has not been determined by the United Kingdom government as ensuring an adequate level of protection for personal data.

**Shared Personal Data**: the personal data to be shared between the Parties under this Agreement. Annex 1 sets out further details relating to the Shared Personal Data, including the types of personal data and categories of data subjects.

1. **DATA PROTECTION**
   1. Each Party shall in relation to the processing of the Shared Personal Data comply with all the obligations imposed on a controller under the Data Protection Legislation, and any material breach of the Data Protection Legislation by one Party shall, if not remedied within thirty (30) days of written notice from the other Party, give grounds to the other Party to terminate this Agreement with immediate effect.
   2. Each Party shall comply with the Data Protection Legislation in processing the Shared Personal Data and shall do all things reasonably necessary to assist the other in complying with its obligations under Data Protection Legislation in respect of the Shared Personal Data. In particular, each Party shall:
      1. ensure that it has in place appropriate technical and organisational measures to protect against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, Shared Personal Data;
      2. ensure that it has all necessary notices and consents in place to enable lawful transfer of the Shared Personal Data to the other Party for such purposes as the Parties have mutually agreed, and consult with the other Party about any notices given to data subjects in relation to the Shared Personal Data wherever possible;
      3. provide the other Party with reasonable assistance in complying with any data subject access request or deletion requests and queries or complaints made under Data Protection Legislation;
      4. provide the other Party with reasonable assistance in ensuring compliance with its obligations under the Data Protection Legislation with respect to security, breach notifications, impact assessments and consultations with supervisory authorities or regulators;
      5. notify the other Party without undue delay on becoming aware of any Personal Data Breach in relation to Shared Personal Data which it has received from the other Party and provide assistance to the other Party as is necessary upon reasonable request to facilitate the handling of any such Personal Data Breach in an expeditious and compliant manner;
      6. maintain complete and accurate records and information to demonstrate compliance with this Agreement;
      7. ensure the reliability of any of its Personnel who have access to personal data and ensure that such Personnel have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
      8. not transfer any Shared Personal Data which it has received from the other Party internationally or to an international organisation except as permitted in accordance with the Data Protection Legislation.
2. **INDEMNITY**
   1. The Data User shall indemnify on demand and keep indemnified Oxford from and against any losses, liabilities, damages, costs, and expenses howsoever arising (including any direct, indirect or consequential losses, loss of profit, loss of reputation and all interest, penalties and legal costs (calculated on a full indemnity basis) and all other reasonable professional costs and expenses) suffered or incurred by Oxford arising out of or in connection with, awarded against, or agreed to be paid by, Oxford pursuant to a claim, action or challenge made by a Data Subject against Oxford, in each case to the extent arising as a result of a breach by the Data User (or its permitted sub-contractors) of this Agreement and/ or their respective obligations under the Data Protection Legislation.
3. **TRANSFERS**
   1. In respect of any Relevant Transfer of Personal Data under this Agreement, the Relevant Transfer shall be governed by Version B1.0 of the International Data Transfer Addendum to the EU SCCs issued by the UK Information Commissioner under s119A(1) of the Data Protection Act 2018, in force 21 March 2022 (the “**IDTA**”). In the event of a conflict between the IDTA and the rest of this Agreement, the terms of the IDTA shall take precedence.
      1. For the purpose of Table 1 of the IDTA:
         1. the start date shall be the Effective Date;
         2. Oxford shall be the Exporter and the Data User shall be the Importer; and
         3. the Parties’ details are as set out on page 2 of this Agreement, and their key contacts are as set out in Annex 1.
      2. For the purpose of Table 2 of the IDTA:
         1. module 1 of the Approved SCCs shall apply; and
         2. clause 7 and the option in clause 11 shall not apply.
      3. The information required for Table 3 is set out in Annex 1.
      4. For Table 4 the Parties select the option that neither Party may end the IDTA when a version is issued by the ICO.

**Annex 1**

**The Approved Research**

As described in the Approved Application.

**Role of the Parties**

The parties have considered the nature of their use of the Approved Research Personal Data and agree that they are independent controllers of the Approved Research Personal Data when it is processed for the purposes of the Approved Research.

**Data Protection Particulars**

|  |  |
| --- | --- |
| **The subject matter and duration of the Processing** | As described in the Agreement and the Approved Application |
| **The nature and purpose of the Processing** | As described in the Agreement and the Approved Application |
| **The categories of Data Subjects** | The individuals who have agreed to participate in the China Kadoorie Biobank study. |
| **The type of Personal Data being Processed** | The Participant Level Data to be processed concern the following categories of personal data:  ·         CSIDs – the encoded and unique pseudonymised study identifiers, which are specific to the Research; and  ·         data derived from questionnaire responses and interviews which do not contain special category data, such as birthplace, early life and education, employment history, marital status and number of children.  Special categories of data  The Participant Level Data to be processed concern the following special categories of data:  The CKB resource contains health, biometric data, and other special category data. All special categories of data contained in the Materials is de-identified (the direct and indirect identifiers are removed).  The types of special category of data may include:  ·         measures of the Participant’s phenotype, such as height, weight and blood pressure.  ·        biomarkers created by assay of the Participant’s samples, which include common biomarkers (such as cholesterol), infectious disease markers, proteomic and metabolomic markers;  ·        data derived from health record linkages including hospital records, death and disease registries or any other sources of clinical data; and  ·        other special category data derived from baseline and resurvey questionnaire responses and interviews, such as past illness / disease history, dietary, cognitive and physical measures. |

**Relevant Transfer Details**

**CONTACT DETAILS OF PARTIES**

Data exporter (Oxford):

Contact person’s name, position and contact details: [this should be the contact person for data queries for the Approved Research]

Data importer (the Data User):

Contact person’s name, position and contact details: [this should be the contact person for data queries for the Approved Research]

**DESCRIPTION OF TRANSFER**

|  |  |
| --- | --- |
| **Categories of data subjects whose personal data is transferred** | [This may be the same as in the data protection particulars section] |
| **Categories of personal data transferred** | [this is a description of the data **actually transferred**, e.g. names, contact details, information about individuals’ health, photographs, recordings, medical scans, dates of birth, etc. It may be the same as the description in the data protection particulars section] |
| **Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.** | [ identify if any of the following categories of data will be transferred, and, if so, any additional security measures in place: racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data for the purpose of uniquely identified a natural person, data concerning health or a person’s sex life or sexual orientation] |
| **Frequency of the data transfer** | [e.g. one-off, monthly, continuous] |
| **Purpose of the transfer and further processing** | [how will the data recipient be processing the data?] |
| **Period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period** |  |

**TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA**

**Definitions**

In this Annex the following terms shall have the meaning set opposite them, unless the context requires otherwise.

|  |  |
| --- | --- |
| **Data** | All Information Processed by the Data User or its Subcontractors in connection with the Agreement. |
| **the Data User Personnel** | Any employee, Subcontractor or agent (including the employees of such Subcontractor or agent) of the Data User engaged by the Data User to provide any part of the Approved Research. |
| **Information** | Information stored in any form, including digital form (e.g. data files stored on electronic or optical media), material form (e.g. on paper), as well as intangible information in the form of employee knowledge. |
| **Information Security** | Preservation of confidentiality, integrity and availability of Information. |
| **Information Security Management System (ISMS)** | Consists of the policies, procedures, guidelines, and associated resources and activities, collectively managed by an organisation, in the pursuit of protecting its Information. |
| **Site** | Any location utilised by the Data User in carrying out the Approved Research (as agreed with Oxford) including but not limited to the Data User’s sites and any other location where Oxford Information is processed. |
| **Subcontractor** | Any contractor appointed by the Data User in accordance with the Agreement to provide all or part of the Approved Research. |

**1 Information security management requirements**

1.1 The Data User shall operate and maintain a recognisable Information Security Management System that is supported by senior management and monitored for effectiveness.

1.2 The Data User shall maintain Information Security policies, supported by topic specific procedures, standards and guidance, which are approved by management, communicated to all employees and relevant third parties and reviewed at least annually.

1.3 the Data User shall operate an Information Security risk assessment process which establishes criteria for analysis, risk treatment, and identifies risk owners and information assets.

1.4 The Data User shall identify and assign specific roles and responsibilities for Information Security and nominate a specific point of contact for Information Security.

1.5 The Data User shall carry out regular independent Information Security reviews of its organisation and infrastructure and act upon the findings.

1.6 The Data User shall make audit reports available to Oxford.

**2 Human resources requirements**

2.1 The Data User shall undertake pre-employment screening of all the Data User Personnel engaged in the Approved Research.

2.2 The Data User shall ensure that pre-employment screening processes obtain or cover:

2.2.1 a minimum of two references from previous employment or education;

2.2.2 validation of previous employment periods and gaps in employment;

2.2.3 criminal records checks; and

2.2.4 validation that educational and training qualifications are legitimate.

2.3 The Data User shall arrange and annually repeat compulsory Information Security awareness training to ensure staff with access to the Data fully understand their Information Security responsibilities.

2.4 The Data User shall maintain and operate a disciplinary policy that defines breaches of security and the possible consequences of misconduct.

**3 Subcontractor requirements**

3.1 The Data User shall provide details of all Subcontractors involved in the delivery of the Approved Research and shall inform Oxford of any changes to Subcontractors.

3.2 The Data User shall maintain written agreements with Subcontractors used to support delivery of the Approved Research that state the Subcontractors’ responsibilities to comply with the security controls and requirements set out in this Schedule.

**4 Information lifecycle management requirements**

4.1 The Data User shall not perform the Approved Research from locations other than the agreed Sites, without obtaining the prior written consent of Oxford.

4.2 The Data User shall only transfer Oxford Information via secure encrypted solutions which have been agreed with Oxford. Encryption solutions shall be compliant with all relevant agreements, laws, and regulations.

4.3 The Data User shall operate secure key management processes for the entire lifecycle of any cryptographic keys.

4.4 The Data User shall ensure that the Data and systems are segregated from other data and systems.

4.5 The Data User shall protect the Data in transit using strong encryption.

4.6 The Data User shall not use the Data in development and/or testing environments without the prior written agreement of Oxford.

4.7 The Data User shall use separate development and/or testing environments from those environments processing or storing the Data.

4.8 The Data User shall ensure that backups of the Data are secured to the same degree as live Data, and are encrypted and securely transported when remotely stored.

4.9 The Data User shall periodically test backups to ensure that Oxford Information can be restored to an operationally acceptable level.

4.10 The Data User shall ensure that, upon planned or unplanned termination of the Agreement, the Data is returned in an agreed form and any other copies are securely destroyed.

4.11 The Data User shall ensure any technologies that have been used to process Oxford Information in the delivery of the Approved Research and are no longer required are securely sanitised or destroyed.

**5 Mobile device requirements**

5.1 The Data User shall ensure that any mobile devices which are used to process or store the Data and/or to connect to systems which process or store the Data have appropriate controls in place, including:

5.1.1 the Data User shall protect such mobile devices with a PIN or passphrase;

5.1.2 the Data User shall configure such mobile devices to ensure they automatically lock after a period of inactivity;

5.1.3 the Data User shall install only trusted applications on such mobile devices;

5.1.4 the Data User shall encrypt such mobile devices; and

5.1.5 the Data User shall implement a process for revoking access to mobile devices and/or other user accounts in the event of loss or theft.

**6 Access control requirements**

6.1 The Data User shall establish, document and maintain a procedure for the provision and limitation of access to Oxford Information and associated systems to those the Data User Personnel who need access to such Information or systems to perform their duties.

6.2 The Data User shall prevent unauthorised access to the Data User and Oxford systems by prohibiting all access by default and explicitly allowing only authorised access.

6.3 The Data User shall ensure that access requests to systems that process Oxford Information are authorised and that there is a valid business reason for the request.

6.4 The Data User shall apply the ‘principle of least privilege’ when allocating access to Oxford Information.

6.5 The Data User shall operate and maintain a user account password policy to ensure that passwords are at least 12 characters in length or have at least equivalent strength or complexity.

6.6 The Data User shall regularly review all accounts and privileges and revoke accounts and privileges which are no longer required.

6.7 The Data User shall ensure that access to Oxford Information and associated systems is logged and auditable so that it can be traced to an individual.

6.8 The Data User shall ensure that audit logs recording user and administrator activities, exceptions and security events are kept for at least ninety (90) days.

6.9 The Data User shall ensure that remote support access is controlled using the following controls:

6.9.1 strong authentication;

6.9.2 access via a secure gateway (e.g. a firewall);

6.9.3 remote support accounts that are only enabled for the duration of the required activity; and

6.9.4 all remote support activity is logged and reviewed.

**7 Operational security and vulnerability management requirements**

7.1 For all technologies used by the Data User to deliver the Approved Research, the Data User shall:

7.1.1 Run antivirus software on all systems commonly affected by malware;

7.1.2 Keep antivirus software up-to-date and configured to perform periodic scans; and

7.1.3 Configure antivirus software to detect and remove all known types of malware.

7.2 For systems not currently considered vulnerable to malware the Data User shall periodically review malware threats to determine whether such systems may require antivirus software.

7.3 The Data User shall develop and use system and software configuration standards, consistent with industry accepted hardening standards, for all systems and technologies used to deliver the Approved Research.

7.4 For all systems and technologies used to deliver the Approved Research, the Data User shall:

7.4.1 Establish a process to identify security vulnerabilities;

7.4.2 Assign specific risk rankings to newly discovered vulnerabilities;

7.4.3 Apply security updates, or other mitigations, on a prioritised basis and within a defined timeframe; and

7.4.4 Apply critical security updates or implement appropriate workarounds within five (5) working days of discovery.

7.5 The Data User shall, at their own cost, perform regular (at least quarterly) vulnerability scans on all of the Data User’s IP addresses (internal / external) that process Oxford Information.

7.6 The Data User, at their own cost, shall arrange for independent annual security penetration testing on internet facing services, relating to the Approved Research.

7.7 Web applications, relating to the Approved Research, shall be tested against OWASP criteria (https://www.owasp.org/) to ensure that they are not vulnerable to the OWASP top ten risks as a minimum requirement.

7.8 The Data User shall implement and document formal change control procedures which are reviewed and updated at least annually and after any significant changes.

**8 Systems and software development requirements**

8.1 For all systems and applications developed for the delivery of the Approved Research the Data User shall:

8.1.1 Operate and maintain a formal systems development lifecycle that incorporates secure engineering principles;

8.1.2 Ensure that applications are developed in a secure development environment including people, processes and technology associated with system development;

8.1.3 Ensure that application developers are trained in secure coding techniques;

8.1.4 Use secure coding guidelines to provide appropriate protection against common vulnerabilities (e.g. the OWASP Guide);

8.1.5 Ensure that all user input is validated for all input fields to protect against common attacks (e.g. SQL injection);

8.1.6 Ensure that contractual arrangements are in place to enforce supervision and monitoring of any outsourced software development;

8.1.7 Operate a process to regularly review code and applications in order to identify security vulnerabilities;

8.1.8 Ensure that changes to code and applications are tested for security impact prior to release; and

8.1.9 Ensure that newly discovered vulnerabilities are assigned an appropriate risk ranking and that security patches are released within a defined period of time following discovery.

**9 Incident detection and management requirements**

9.1 The Data User shall monitor security breaches based on policies which allow for alerting of critical events to security administrators.

9.2 The Data User shall implement intrusion detection systems where internet connections exist.

9.3 The Data User shall maintain and operate a security incident response process that ensures that incidents impacting or having the potential to impact the Data are adequately managed, including:

9.3.1 Immediate reporting of such incidents to Oxford;

9.3.2 Isolation of systems which are known to be compromised; and

9.3.3 Investigation and mitigation of the root-cause of such incidents before taking systems back online following an incident.

**10 Physical security requirements**

10.1 The Data User shall provide and maintain suitable accommodation, facilities, equipment, furnishing, utilities and fixtures necessary to provide secure physical premises that provide a safe working environment and which adequately protect against loss or damage to the premises or anything therein, including:

10.1.1 the Data User shall define security perimeters to protect such areas;

10.1.2 the Data User shall ensure that appropriate intruder detection systems are installed;

10.1.3 the Data User shall restrict physical access to such areas;

10.1.4 the Data User shall ensure that access to such areas is monitored and recorded;

10.1.5 the Data User shall ensure that access is restricted to authorised personnel only;

10.1.6 the Data User shall ensure that access by visitors to such areas is appropriately recorded and that visitors are supervised at all times;

10.1.7 the Data User shall implement protection against physical and environmental threats (e.g. fire, water, dust); and

10.1.8 the Data User shall ensure that utilities servicing such areas (e.g. electricity, water or ventilation) are protected against failure and disruption.

**11 Right to audit**

11.1 The Data User shall allow Oxford or its agent or representative at all reasonable times and on reasonable notice to enter Sites used by the Data User in connection with the provision of the Approved Research for the purpose of auditing the compliance of the Data User with its obligations under this Schedule.

11.2 The Data User shall ensure that all the Data User Personnel cooperate with such audits and, if requested, shall make relevant the Data User Personnel available for interview.