Data Sharing Agreement

1. Agreement

1.1 This Data Processing Agreement ("Agreement") is

BETWEEN

1) **University College London Hospitals NHS Foundation Trust (UCLH)**, of Trust Headquarters**,** 250 Euston Road London NW1 2PG, (hereinafter known as **"the controller"**) AND

2) **University College London** whose registered office is at **Gower Street, London, WC1E 6BT** (hereinafter referred to as '**the processor**').

Collectively the "Parties" and each individually a "Party".

1.2 Throughout this Agreement the singular is not intended to exclude the plural, nor either gender the other. Where such expressions are used the wording is to be interpreted to include the alternatives unless expressly excluded. Words denoting persons include corporations and vice versa.

1.3 This Agreement sets out the responsibilities of each Party in respect of the NHS Information as defined in Clause 2 below.

2. Definitions

2.1 Throughout this Agreement the following terms shall be taken to have the following meanings unless expressly stated otherwise:

Agreement:	Unless explicitly stated otherwise refers solely to this Data Processing Agreement including any appendices and schedules
Data:	Includes 'Personal Data' and 'Sensitive Personal Data' along with any data generated through this Agreement
Data Controller:	Shall have the definition ascribed in Article 4(7) UK GDPR
Data Processor:	Shall have the definition ascribed in Article 4(8) UK GDPR
Data Subject:	Shall have the definition as contained within Article 4(1) UK GDPR
DPA:	Data Protection Act 2018
EIR:	Environmental Information Regulations 2004
FOIA:	Freedom of Information Act 2000
Intellectual Property:	shall mean patents, trademarks, service marks, registered designs, copyrights, database rights, design rights, rights in respect of

	confidential information, applications for any of the above, and any similar right recognised from time to time in any jurisdiction, together with all rights of action in relation to the infringement of any of the above.
UK GDPR:	UK General Data Protection Regulation
Personal Data:	Shall have the definition ascribed in Article 4(1) UK GDPR
Personnel:	Individuals employed by, contracted to or otherwise with a legitimate business reason to access Data owned or processed on behalf of either Party, regardless of whether or not a contract exists between the Party and the relevant individual(s)
Sensitive Personal Data:	Shall have the definition of 'special categories of personal data' ascribed in Article 9(1) UK GDPR

3. Purpose

To allow UCLH **University College London Hospitals NHS Foundation Trust** to provide anonymised data extracted from medical devices and existing databases to the CHIMERA research data base hosted in the **University College London** Data Safe Haven.

4. Scope

University College London Hospitals NHS Foundation Trust will provide anonymised data extracted from medical devices and existing databases to the Collaborative Healthcare Innovation through Mathematics, EngineeRing and AI (CHIMERA) research database hosted in the **University College London's Data Safe Haven.**

Personal data other than (rounded) age and gender will *not* be extracted. The research database protocol has been reviewed by NHS Research Ethics Committee (East Midlands – Derby) on 6 July 2021 (reference 21/EM/0134) and is designed to meet the standards laid out in the Information Commissioner's Office Anonymisation Code of Conduct.
Data flows will be merged from:

1. Integrated electronic health record systems (EHRS). This is currently provided by Epic Health Systems at University College Hospital.
2. Legacy data from previous clinical information systems (CIS).
3. Device specific information that is not processed by the EHRS or CIS. This would include patient monitoring systems (e.g., cardiac monitors, wearable devices etc.), near patient testing devices (e.g., blood gas machines), and treatment devices (e.g., ventilators and haemofilters).

4.2 This Agreement is not designed or intended to cover any other data sharing or processing between the Parties. Other such work must be covered under separate agreements and or legal bases.

5. Roles and Responsibilities

5.1 For the purpose of this Agreement, UCLH is the Data Controller and the Data Processor (in that UCLH is preparing the anonymised extract for transfer to UCL).
University College London *(in concept only)* is also a Data Processor. We use the term '*in concept only*' parenthetically to emphasise that these data are no longer personal data because they have been anonymised and therefore outside the scope of the Article 4(8) UK GDPR.

6. Data Sharing / Processing & Legal Basis

6.1 Data will be shared and processed under the terms of this Agreement.

6.2 It is the responsibility of both Parties to ensure they have a legal basis for the processing to be carried out. It is anticipated that normally one or many of the following bases will apply however there is nothing to prevent other valid legal bases being identified and utilised:

Please delete below appropriate
Article 6 (e) Public task: the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

Article 9(2) (j) Archiving, research, and statistics (with a basis in law): processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject

Article 9(3): Personal data referred to in paragraph 1 (Article 9(1)) may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies

7. Confidential Information/Data

7.1 Confidential information/ data means all confidential information relating to the Purpose for which the Discloser, its Representatives, Group Companies, or their Representatives directly or indirectly discloses, or makes available, to the Recipient, its Representatives, its Group Companies, or their Representatives, before, on, or after the date of this agreement.

This includes:

- the purpose and status of discussions and negotiations between the parties
  all confidential or proprietary information relating to:
    - the business, affairs, properties, assets, personnel, customers, clients, suppliers plans, intentions, or market opportunities of the Discloser or of any of the Discloser's Group Companies; and

- the operations, processes, product information, know-how, technical information, designs, trade secrets or software of the Discloser, or of any of the Discloser's Group Companies;
- all personal data and Special category data (within the meaning of the Data Protection Act (DPA) 2018 that encompasses the definition as set out in the General Data Protection Regulation (UK GDPR) 2016) of the Discloser under clause 9 of this agreement;
- any information, findings, data or analysis derived from Confidential Information;
- any other information that is identified or ought reasonably to be considered as being of a confidential or proprietary nature;
-

7.2 Information shared under this agreement will not be considered Confidential Information where:

- it is, or becomes, generally available to the public and is not a direct or indirect result of a breach of this agreement by the Recipient, its Representatives, it's Group Companies or any of their Representatives in breach of this agreement;
- it was available to the Recipient on a non-confidential basis prior to disclosure by the Discloser;
- it was, is, or becomes available to the Recipient on a non-confidential basis from a person who, to the Recipient's knowledge, is not under any confidentiality obligation in respect of that information;
- it was lawfully in the possession of the Recipient before the information was disclosed by the Discloser;
- it is developed by or for the Recipient independently of the information disclosed by the Discloser; or the parties agree in writing that the information is not confidential.

8. Intellectual property

8.1 The Data remains the property of the Disclosing Party. To avoid any doubt any UCLH Data shall remain the property of UCLH.

8.2 Other than as explicitly set out in this Agreement, nothing in this Agreement shall be construed so as to grant the Receiving Party any licence or right (a) in respect of any Confidential Information of UCLH or (b) under any Intellectual Property comprised in or that otherwise protects any such Confidential Information.

8.3 The Receiving Party shall remove any proprietary, copyright, trade secret, confidentiality or other notice from any Confidential Information of any Disclosing Party.

9. Data Security

Technical

9.1 In terms of Data collected or created going forward, the processor shall segregate the Data held within the IT systems utilised. Data shall be transitioned within the same network or using at least AES 256 bit encryption.

9.2 Data Privacy Impact Assessment must be completed between the controller and processor and sent to the controller's Information Governance for approval.

9.3 Data shall be segregated using logical or physical separation, but it shall not be possible for a user to transition between two systems.

9.4 the processor shall ensure technical controls are in place to prevent unauthorised access to the Data and which protect the confidentiality, integrity and availability of the Data.

9.5 the processor shall conduct appropriate testing, vulnerability scans, and risk management, through to firewalls, enforcing strong passwords and third-party due diligence in line with article 32 of the UK GDPR as part of its routine testing schedules to ensure the Data remain secure within its network. Should the Data be hosted by an external supplier, the processor shall be responsible for ensuring tests are conducted by the supplier on a regular basis to ensure the continued security of the Data.

9.6 Upon request, the processor shall provide the controller with documented assurance that adequate controls are in place to offered continued protection for the data which meets NHS standards at the time.

9.7 The processor shall ensure that appropriate role-based access controls are in place to ensure only those Personnel with a business need to access Data are able to do so. Further roles shall be defined to ensure that those with permission to access Data are only able to see Data relevant to their function and not the entire user base unless such access is appropriate.

Physical

9.8 The processor shall deploy appropriate physical controls to ensure only those with a business need are able to access assets containing or accessing the controller Data.

9.9 The processor shall ensure physical controls protect both electronic data and that held in a manual format.

9.10 The processor shall ensure that physical controls are tested on a regular (at least annually) basis to ensure they remain effective

9.11 Any defects identified in physical controls shall be rectified as soon as possible. If control defects cannot be rectified and leave data open to risk of breach of confidentiality, integrity and or availability the processor shall put in place any additional measures necessary to ensure the continued security whilst the defect is remedied.

Procedural

9.12 The processor shall put in place procedural controls to ensure Data is not exposed to risk of compromise of confidentiality, integrity and availability.

9.13 The processor shall make all appropriate Personnel aware of the procedural controls in place and carry out checks where appropriate to ensure Personnel must comply with their responsibilities.

Breaches

9.14 Any breach or attempted breach of the confidentiality, integrity, availability or overall security of the Data must be reported to the controller electronically within twenty-four (24) hours of them becoming aware of the incident or near miss.

9.15 Immediately upon becoming aware of an incident or near miss, the processor shall take all practicable and reasonable steps to prevent further harm or risk of harm to the Data.

9.16 The processor shall immediately commence an investigation into the cause of the breach and take steps to prevent it occurring again.

9.17 Should there be a requirement to report the incident to a regulator such as the Information Commissioner; the processor shall provide the controller with all relevant information and provide full support and assistance in this case.

9.18 Should an investigation be carried out into the incident by a third-party regulator, the processor shall provide the controller with all necessary and reasonable assistance to enable the controller to respond to and comply with the requirements of the investigation.

9.19 Should there be a requirement for the controller to contact Data Subjects to notify them of a breach, the processor shall provide reasonable assistance to the controller to facilitate this being completed with appropriate expediency.

Remote/Mobile Devices

9.20 As part of the processing it is likely data will be accessed but not stored on mobile/tablet devices during working from home measures. Storage of Data on mobile devices shall be subject to written authorisation from for specific purpose(s).

9.21 The controller Data may not otherwise be held on mobile devices which are not owned by the controller. the controller devices are secured under a mobile device management policy.

10. Data Subject Rights

10.1 Under DPA and UK GDPR, Data Subjects have a number of rights which can be exercised against the Data Controller.

10.2 Should the controller receive a request in respect of the exercise of Data Subject rights which covers data being held on its behalf by the processor, the processor shall provide all necessary reasonable assistance in carrying out the requirements of the controller to enable compliance with the requirements of the law.

10.3 Should the processor receive a request to exercise Data Subject rights in respect of Data for which it is the Data Processor, it shall forward the requester on to the controller

11. Freedom of Information

11.1 Both Parties to this Agreement are considered public authorities as defined within the FOIA and are therefore subject to the provisions of that Act and the EIR.

11.2 Should the processor receive a request under either FOIA or EIR concerning the Data for which it is a Data Processor it shall direct the requester to the controller or offer to transfer the request to the controller in accordance with its own standard procedures.

11.3 Only in circumstances where the processor has explicit written permission from the controller to respond on its behalf may the processor respond to a request received or directed to the controller.

11.4 Data which has been shared under this Agreement and for which the processor has become the Data Controller shall be the responsibility of the processor.

11.5 In circumstances where requests are received concerning matters handled under this Agreement, the Parties shall seek to notify each other of the request in order that both are aware of matters which may arise in the public domain.

12. Audit

12.1 The controller has the right to audit the processor compliance with the terms of this Agreement.

12.2 Additional audit is permitted should a breach of this Agreement by the processor or any of its contractors, staff, parties etc. occur, regardless of whether or not it has been reported to the controller or come to the controller's attention by other means.

13. Subcontractors

13.1 For the purpose of processing the controller Data, the processor may subcontract the responsibility without the prior written consent of the controller, and the processor may use third parties for IT provision. Potential third parties may include, and may not be limited to*: Amazon Web Servers (AWS)*

13.2 Any contracted-out provision provider must be subject to at least the same conditions as contained herein to ensure the security of the data and confidentiality remains protected.

14. Liability

14.1 The Processor agrees to indemnify and keep indemnified and defend at its own expense the Controller against all costs, claims, damages or expenses incurred by the Controller or for which the Controller may become liable due to any failure by the Processor or its employees or agents to comply with any of its obligations under this Agreement.

14.2 The Controller agrees to indemnify and keep indemnified and defend at its own expense Processor against all costs, claims, damages, fines, penalties or expenses (including without limitation fines and penalties imposed by the Information Commissioner Office) incurred by

Processor or for which the Processor may become liable, due to any failure by the Controller or its employees or agents to comply with any of its obligations under this Agreement.

15. Legal Jurisdiction

15.1 This Agreement is governed by and shall be interpreted in accordance with the law of England and Wales.

15.2 In the event of a dispute, the parties to this Agreement agree to attempt to resolve such issues according to NHS dispute resolution procedures. In the event that agreement cannot be reached, the parties agree that the courts of England and Wales shall have exclusive jurisdiction to hear the case.

16. Review and Duration of Agreement

16.1 This Agreement shall be reviewed by the Parties at least annually to ensure it remains fit for purpose and that the purpose and or scope has not altered.

16.2 Reviews may be carried out at any such time as either Party identifies the possibility or need for a material change to the content herein.

16.3 This Agreement shall remain in force until such time as the notice to terminate is provided by either Party.

17. Notices and Amendments

17.1 Minor amendments may be made to this Agreement at any time on the written agreement of the Parties.

17.2 Should a number of changes be required or any change which fundamentally alters the Purpose of this Agreement be proposed the Parties will review the entire Agreement and negotiate accordingly.

17.3 Should the controller deem any change likely to breach its obligations as a Data Controller its position is final and may only be challenged through the courts of England and Wales.

17.4 Each Party will notify the other in writing at the commencement of this Agreement of the person / role within their organisation who is authorised to negotiate amendments. Only that individual or their notified replacement may negotiate and approve changes, subject to any additional internal requirements of the Party.

18. Agreement and Signatures

18.1 The Parties hereby agree to be bound by the terms and conditions stated in this Agreement. In signing this Agreement, the Parties acknowledge their respective responsibilities and that those signing are duly authorised by their relevant organisations to do so.

18.2 In the event of any term in this Agreement or any part thereof being declared invalid or unenforceable, all other terms and parts thereof shall remain fully in force and effect and shall not be affected thereby.

18.3 The failure of either Party at any time to enforce any of the provisions of this Agreement or to require performance of any of the provisions of the Agreement shall in no way affect its right thereafter to require complete performance by the other Party, nor shall any waiver of any breach of any provision be taken or held to be a waiver of any subsequent breach of any provision or be a waiver of the provision itself.

Signatures

On behalf of **University College London Hospitals NHS Foundation Trust**:

Signature: 

Name: Dr Gee Yen Shin

Role: Caldicott Guardian

Date: 27th June 2022

Business Address: University College London Hospitals NHS Foundation Trust
250 Euston Road
London
NW1 2PG

On behalf of **University College London**

Signature: Y. Baveas

Name: Yanni Baveas

Role: Senior Contracts Manager

Date: 26th January 2023

Business Address: Gower St, London WC1E 6BT