

Population Health Management Development Programme

Using

**De-identified General Practice primary care data
and
De-identified CCG commissioning data**

Data Processing Agreement

between

- (1) **The Mid and South Essex STP CCGs**
- (2) **The participating General Practices of the Mid and South Essex
STP CCGs**
- and
- (3) **Optum Health Solutions (UK) Limited**

April 2021

This Agreement will be executed in counterparts – it will be signed separately by each participating organisation. Each counterpart shall be deemed to be an original document and all of the counterparts taken together shall constitute one single agreement between the participating organisations.

Introduction

The CCGs of the Mid and South Essex Sustainability Transformation Partnership (STP):

- **NHS Basildon & Brentwood CCG**
- **NHS Castle Point & Rochford CCG**
- **NHS Mid Essex CCG**
- **NHS Southend CCG**
- **NHS Thurrock CCG**

and their member General Practices at a PCN level, are working with NHS England and Improvement, the North of England Commissioning Support Unit (NECS) and Optum to deliver a Population Health Management Development Programme (Hereafter referred to as the Programme).

The overall purpose of the Programme is an intensive 20-week programme designed to support PCNs to redesign care based on data-driven insights, and to use their learning at local level to accelerate understanding of health and care needs, and development of PHM infrastructure, at system / place / neighbourhood level. This will be achieved using data flowing into Arden & GEM CSU under the previously signed Population Health Management and Risk Stratification Data Sharing and Data Processing Agreement.

Population health management is described by NHS England as the analysis and segmentation of the needs of a population and the design of clinical and other interventions to prevent illness or acute deterioration. Participating organisations will be able to improve health outcomes for selected local population groups through the real-time application of intelligence-led care design.

Population health management is not a new concept, but it is yet to be consistently implemented in systems across England.

A core component of the Programme is the creation of a linked data set that serves as ‘the single source of truth’. This enables teams from a variety of sectors and levels within the system to share an objective common language built on the actual needs of the people they jointly serve. Through the programme, the HCP will receive a set of tailored analytics that can inform decisions from system planning through to individual patient care. The change that happens within PCNs will help system leadership learn how to best enable and unblock PHM interventions, in order to scale and ultimately catalyse new ways of working across the HCP.

Participation in this Programme will support General Practices and CCGs in meeting their contractual obligations that arise from the NHS Long Term Plan.

It is important to note that the Programme only provides Optum as Data Processor, with access to de-identified record level or aggregate data. NO personal confidential data (PCD) will be available to anyone within Optum.

Optum is engaged in the capacity of a **data processor** to each participating organisation (i.e. to those General Practices and CCGs that have signed this Agreement).

THIS AGREEMENT (the “Agreement”) is made on 14 April 2021 (the “Effective Date”).

BETWEEN:

NHS Basildon & Brentwood CCG, NHS Castle Point & Rochford CCG, NHS Mid Essex CCG, NHS Southend CCG and NHS Thurrock CCG (the Mid and South Essex STP CCGs), The participating General Practices of the Mid and South Essex STP CCGs (together referred to as the Data Controllers);

and Optum Health Solutions (UK) Ltd with registered office at 10th Floor, 5 Merchant Square, London W2 1AS (“Data Processor”, “Processor” or “Optum”);

BACKGROUND

- a) The Mid and South Essex STP CCGs have appointed a Data Processor to perform the processing of the Population Health Management Development Programme on behalf of participating General Practices under the terms of this Agreement.
- b) The Data Controllers shall provide instructions with regard to the processing of Pseudonymised data to the Data Processor.
- c) In performing the Services, the Data Processor is required to process certain pseudonymised data (as defined in Annex 1 & 2). The Data Controllers have agreed to provide such pseudonymised data to the Data Processor for processing only in accordance with the terms of this Agreement from the Effective Date.
- d) Arden and Gem CSU will provide the data to the Data Processor on behalf of the Data Controllers.
- e) In consideration of the Mid and South Essex STP CCGs engaging the services of the Data Processor to process pseudonymised data on behalf of its Beneficiaries the Data Processor shall comply with the security, confidentiality and other obligations imposed on it under this Agreement.

IT IS AGREED as follows:

1 DEFINITIONS AND INTERPRETATION

1.1 The following definitions shall apply in this agreement:

Agreement shall mean this Data Processing Agreement entered into at the date stated above;

Anonymised Data means strip Personal Data of sufficient elements that means the individual can no longer be identified this must be carried out in line with the ICO code of practice

Data Controller shall take the meaning given in the Data Protection Legislation;

Data Guidance means any applicable guidance, guidelines, direction or determination, framework, code of practice, standard or requirement regarding information governance, confidentiality, privacy or compliance with the Data Protection Legislation (whether specifically mentioned in this Contract or not) to the extent published and publicly available or their existence or contents have been notified to the Processor by The Data Controller and/or any relevant Regulatory or Supervisory Body. This includes but is not limited to guidance issued by NHS Digital, the National Data Guardian for Health & Care, the Department of Health, NHS England, the Health Research Authority, Public Health England, the European Data Protection Board and the Information Commissioner;

Data Loss Event means any event that results, or may result, in unauthorised processing of Personal Confidential Data held/accessed by the Data Processor under this Agreement or that that the Processor has responsibility for under this Agreement including without limitation actual or potential loss, destruction, corruption or inaccessibility of Personal Data including any Personal Data Breach.

Data Processing Services means the data processing services described in each Annex to this Agreement;

Data Processor Personnel means any and all persons employed or engaged from time to time in the provision of the Services and/or the processing of Personal Data whether employees, workers, consultants or agents of the Data Processor or any subcontractor or agent of the Data Processor.

Data Protection Impact Assessment means an assessment by the Data Controller of the impact of the envisaged processing on the protection of Personal Data;

Data Protection Legislation means (i) the GDPR, the Law Enforcement Directive (Directive (EU) 2016/680) (LED) and any applicable national Laws implementing them as amended from time to time (ii) the DPA 2018 (iii) all applicable Law concerning privacy, confidentiality or the processing of Personal Data including but not limited to the Human Rights Act 1998, the Health and Social Care (Safety and Quality) Act 2015, the common law duty of confidentiality and the Privacy and Electronic Communications (EC Directive) Regulations

Data Protection Officer shall take the meaning given in the Data Protection Legislation;

Data Subject shall take the meaning given in the Data Protection Legislation;

Data Subject Access Request means a request made by, or on behalf of, a Data Subject in accordance with rights granted pursuant to the Data Protection Legislation to access their Personal Data;

DPA 2018 means Data Protection Act 2018;

EU means the European Union;

European Data Protection Board has the meaning given to it in the Data Protection Legislation;

GDPR means the General Data Protection Regulation (Regulation (EU) 2016/679)

Information Commissioner means the independent authority established to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals and any other relevant data protection or supervisory authority recognised pursuant to the Data Protection Legislation;

Law means any law or subordinate legislation within the meaning of Section 21(1) of the Interpretation Act 1978, bye-law, enforceable right within the meaning of Section 2 of the European Communities Act 1972, regulation, order, regulatory policy, mandatory guidance or code of practice, judgment of a relevant court of law, or directives or requirements with which the Data Processor is bound to comply;

LED means the Law Enforcement Directive (Directive (EU) 2016/680)

LTPS means the NHS Liabilities to Third Parties Scheme as amended or superseded from time to time;

Personal Data/Special Category Data shall take the meaning given in the Data Protection Legislation;

Personal Data Breach shall take the meaning given in the Data Protection Legislation;

Processor shall take the meaning given in the Data Protection Legislation;

Processing and cognate terms shall have the meaning given in the Data Protection Legislation;

Protective Measures means appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data; ensuring confidentiality, integrity, availability and resilience of systems and services; ensuring that availability

of and access to Personal Data can be restored in a timely manner after an incident;
and regularly assessing and evaluating the effectiveness of the such measures;

Pseudonymised Data: Pseudonymisation is a technique that replaces or removes information in a data set that identifies an individual.

Regulatory or Supervisory Body means any statutory or other body having authority to issue guidance, standards or recommendations with which the Processor and/or Data Processor Personnel must comply or to which it or they must have regard, including:

- (i) CQC;
- (ii) NHS Improvement;
- (iii) NHS England;
- (iv) the Department of Health;
- (v) the National Institute for Health and Care Excellence;
- (vi) Healthwatch England and Local Healthwatch;
- (vii) Public Health England;
- (viii) the General Pharmaceutical Council;
- (ix) the Healthcare Safety Investigation Branch;
- (x) Information Commissioner;
- (xi) European Data Protection Board;
- (xii) The Health & Social Care Information Centre (known as NHS Digital)

Services means the data processing activities carried out by Processor as outlined further in each individual Annex;

Sub-processor means another third party data processor appointed by the Data Processor to process Personal Data on behalf of the Data Processor related to this Agreement;

Working Day means a day other than a Saturday, Sunday or bank holiday in England

- 1.2 reference to any legislative provision shall be deemed to include any statutory instrument, bye law, regulation, rule, subordinate or delegated legislation or order and any rules and regulations which are made under it, and any subsequent re- enactment, amendment or replacement of the same;
- 1.3 the Annex forms 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 Annex; and
- 1.4 references to clauses and Annexes are to clauses and Annexes to this agreement.

2 SCOPE OF THIS AGREEMENT

- 2.1 In consideration of the Data Processor agreeing to provide the Services to the Data Controllers, and the Data Controllers agreeing to provide pseudonymised data to Processor, the parties have agreed that from the Effective Date, the terms of this Agreement will apply to and govern all processing of pseudonymised data by the Data Processor.
- 2.2 The Data Processor and the Data Controllers shall both comply with all applicable Data Protection Legislation for the duration of this Agreement and nothing in this Agreement shall relieve either party of these obligations.
- 2.3 The Data Controllers confirm that the Data Processor is not processing Personal Data under this Agreement. The Data Processor receives data on behalf of the Data Controllers from Arden & Gem CSU in a pseudonymised format that meets the requirements of the ICO anonymisation code of practice, the Data Processor does not have access to any information that would enable them to identify an individual and should not seek to re-identify individuals from that data as it has been converted into an anonymised format by Arden & Gem CSU.

3 PROCESSING OF PSEUDONYMISED DATA

- 3.1 The Parties acknowledge that for the purposes of the Data Protection Legislation and the delivery of the Data Processing Services, the Mid and South Essex STP CCGs and General Practices are the Data Controllers and Optum Health Solutions (UK) Ltd is the Data Processor.
- 3.2 The Data Controllers retain control of the pseudonymised data and remains responsible for its compliance obligations under the applicable Data Protection Legislation, including providing any required notices and obtaining any required consents, and for the processing instructions it gives to Processor.

- 3.3 The Data Processor shall notify the Data Controllers immediately if it considers that any of the instructions provided infringe the Data Protection Legislation.

DATA PROTECTION IMPACT ASSESSMENTS

- 3.4 The Data Processor shall provide all reasonable assistance to the Data Controllers in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Data Controllers, include:
- 3.4.1 a systematic description of the envisaged Processing operations and the purpose of the Processing;
 - 3.4.2 an assessment of the necessity and proportionality of the Processing operations in relation to the Data Processing Services;
 - 3.4.3 an assessment of the risks to the rights and freedoms of natural persons; and
 - 3.4.4 mutually agreed upon measures to address the risks, including safeguards, security measures and mechanisms to ensure the protection of pseudonymised data.
- 3.5 The Data Processor shall provide all reasonable assistance to the Data Controllers if the outcome of the Data Protection Impact Assessment leads the Data Controllers to consult the Information Commissioner.

PROTECTIVE MEASURES

- 3.6 The Data Processor shall, in relation to any pseudonymised data processed in connection with its obligations under this Agreement:
- 3.6.1 Process that pseudonymised data only in accordance with the instructions set out in each Annex, unless the Data Processor is required to do otherwise by Law. If it is so required the Data Processor shall promptly notify the Data Controllers before processing the pseudonymised data unless prohibited by Law.
 - 3.6.2 ensure that it has in place Protective Measures, which have been reviewed and approved by the Data Controllers as appropriate to protect against a Data Loss Event having taken account of the:
 - 3.6.2.1 nature of the data to be protected;

- 3.6.2.2 harm that might result from a Data Loss Event;
 - 3.6.2.3 state of technological development; and
 - 3.6.2.4 cost of implementing any measures.
- 3.6.3 ensure that:
- 3.6.3.1 The Processor Personnel do not process the pseudonymised data except in accordance with this Agreement (and in particular each Annex)
 - 3.6.3.2 it takes all reasonable steps to ensure the reliability and integrity of any of the Processor Personnel who have access to the pseudonymised data and ensure that they:
 - 3.6.3.2.1 are aware of and comply with the Processor duties under this clause;
 - 3.6.3.2.2 are subject to appropriate confidentiality undertakings with Processor or any Sub-processor that are in writing and are legally enforceable;
 - 3.6.3.2.3 are informed of the confidential nature of the pseudonymised data and do not publish, disclose or divulge any of the pseudonymised data to any third party unless directed in advance and in writing to do so by the Data Controllers or as otherwise permitted by this Agreement.
 - 3.6.3.2.4 have undergone adequate training in the use, care, protection and handling of pseudonymised data that enables them and Processor to comply with their responsibilities under the Data Protection Legislation and this Agreement. The Data Processor shall provide the Data Controllers with evidence of

completion and maintenance of that training within three Working Days of request by the Data Controllers.

- 3.6.4 not transfer pseudonymised data outside of the EU unless the prior written consent of the Data Controllers has been obtained and the following conditions are fulfilled:
- 3.6.4.1 The Data Controllers or Data Processor has provided appropriate safeguards in relation to the transfer as determined by the Data Controllers;
 - 3.6.4.2 the Data Subject has enforceable rights and effective legal remedies;
 - 3.6.4.3 The Data Processor complies with its obligations under the Data Protection Legislation by providing an adequate level of protection to any pseudonymised data that is transferred (or, if it is not so bound, uses its best endeavours to assist the Data Controller in meeting its obligations) and;
 - 3.6.4.4 The Data Processor complies with any reasonable instructions notified to it in advance by the Data Controllers with respect to the processing of the pseudonymised data.
- 3.6.5 at the written direction of the Data Controllers, delete or return the pseudonymised data (and any copies of it) on termination of the Agreement unless the Data Processor is required by Law to retain the Personal Data. If the Data Processor is asked to delete the pseudonymised data they shall provide the Data Controllers with evidence that the pseudonymised data has been securely deleted in accordance with the Data Protection Legislation within a period agreed within the written direction of the Data Controllers.
- 3.6.6 Any data breach or suspected data breach will be reported to the Data Controllers on discovery.
- 3.6.7 The data processor will cooperate with the Data Controllers where appropriate in responding to FOI requests.

TECHNICAL AND ORGANISATIONAL SECURITY MEASURES

- 3.7 Taking into account, the cost of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, The Data Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including, but not limited to, as appropriate:
- 3.7.1 received pseudonymisation (or if Personal Data is received in pseudonymised form, maintain pseudonymisation) and encryption of Personal Data;
 - 3.7.2 the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
 - 3.7.3 the ability to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident; and
 - 3.7.4 a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of Processing.

SUB-PROCESSOR

- 3.8 Before allowing any additional Sub-processor to process any pseudonymised data related to this Agreement, The Data Processor must:
- 3.8.1 notify the Data Controllers in writing of the intended Sub-processor and Processing;
 - 3.8.2 obtain the written consent of the Data Controllers;
 - 3.8.3 enter into a written agreement with the Sub-processor which gives effect to the terms set out in this Agreement such that they apply to the Sub-processor and in respect of which the Data Controllers are given the benefits of third party rights to enforce the same; and
 - 3.8.4 provide the Data Controllers with such information regarding the Sub-processor as the Data Controllers may reasonably require.

- 3.9 The Data Processor shall ensure that the third party's access to the pseudonymised data terminates automatically on termination of this Agreement for any reason save that the Sub-processor may access the pseudonymised data in order to securely destroy it.
- 3.10 The Data Processor shall remain fully liable for all acts or omissions of any Sub-processor.

SUBJECT ACCESS / RIGHTS REQUESTS

- 3.11 Subject to clause 3.14, The Data Processor shall notify the Data Controllers without undue delay if it:
- 3.11.1 receives a Data Subject Access Request (or purported Data Subject Access Request) connected with Personal Data processed under this Agreement;
 - 3.11.2 receives a request to rectify, block or erase any Personal Data connected with Personal Data processed under this Agreement;
 - 3.11.3 receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation connected with Personal Data processed under this Agreement;
 - 3.11.4 receives any communication from the Information Commissioner or any other Supervisory or Regulatory Body connected with Personal Data processed under this Agreement;
 - 3.11.5 receives a request from any third party for disclosure of Personal Data connected with this Agreement; or
 - 3.11.6 becomes aware an actual or suspected Data Loss Event.
- 3.12 This notification shall be given by emailing the original request and any subsequent communications to the Data Controllers.
- 3.13 The Data Processor shall not respond substantively to the communications listed at clause 3.11 save that it may respond to a Regulatory or Supervisory Body following prior consultation with the Data Controllers.

- 3.14 The Data Processor' obligation to notify under clause 3.11 shall include the prompt provision of further information to the Data Controllers in phases, as details become available.
- 3.15 Taking into account the nature of the processing, The Data Processor shall provide the Data Controllers with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 3.11 (and insofar as possible within the timescales reasonably required by The practice) including by promptly providing:
- 3.15.1 the Data Controllers with full details and copies of the complaint, communication or request;
 - 3.15.2 such assistance as is reasonably requested by the Data Controllers to enable the Data Controllers to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;
 - 3.15.3 such assistance as is reasonably requested by the Data Controllers to enable the Data Controllers to comply with other rights granted to individuals by the Data Protection Legislation including the right of rectification, the right to erasure, the right to object to processing, the right to restrict processing, the right to data portability and the right not to be subject to an automated individual decision (including profiling);
 - 3.15.4 the Data Controllers, at its request, with any Personal Data it holds in relation to a Data Subject;
 - 3.15.5 assistance as requested by the Data Controllers following any Data Loss Event;
 - 3.15.6 assistance as requested by the Data Controllers in relation to informing a Data Subject about any Data Loss Event, including communication with the Data Subject;
 - 3.15.7 assistance as requested by the Data Controllers with respect to any request from the Information Commissioner's Office, or any consultation by the Data Controllers with the Information Commissioner's Office;
 - 3.15.8 the Data Controllers with any copies of requests from Data Subjects seeking to exercise their rights under the Data Protection Legislation. Such requests

must be sent, to the Data Controllers without undue delay, and in no longer than three (3) Working Days of receipt by Processor.

- 3.16 The Data Processor shall allow for reasonable audits of its delivery of the Data Processing Services by the Data Controllers or the Data Controllers designated auditor, on at least 20 Working Days' notice, during the term of this Agreement. Processor will give the Data Controllers all necessary assistance to conduct such audits.
- 3.17 The Data Processor shall provide the Data Controllers with evidence to demonstrate compliance with all of its obligations under this Agreement and the relevant Data Protection Legislation.

DATA PROTECTION OFFICER

- 3.18 The Data Processor shall designate a Data Protection Officer if required by the Data Protection Legislation and shall communicate to the Data Controllers the name and contact details of any Data Protection Officer.

RECORD OF THE DATA PROCESSING ACTIVITIES

- 3.19 The Data Processor shall maintain complete and accurate records and information to demonstrate its compliance with this Agreement, the Data Protection Legislation and Data Guidance. The Data Processor must create and maintain a record of all categories of data processing activities carried out under this Agreement, containing:
- 3.20 the categories of Processing carried out under this Agreement;
- 3.21 where applicable, transfers of pseudonymised data to a third country or an international organisation, including the identification of that third country or international organisation and, where relevant, the documentation of suitable safeguards;
- 3.22 a general description of the Protective Measures taken to ensure the security and integrity of the pseudonymised data processed under this Agreement; and
- 3.23 a log recording the processing of pseudonymised data in connection with this Agreement comprising, as a minimum, details of the pseudonymised data concerned, how the pseudonymised data was processed, where the pseudonymised data was processed and the identity of any individual carrying out the processing.

- 3.24 The Data Processor shall ensure that the record of processing maintained in accordance with clause 3.19 is provided to the Data Controllers within two Working Days of a written request from the Data Controllers.
- 3.25 This Agreement does not relieve the Data Processor from any obligations conferred upon it by the Data Protection Legislation.
- 3.26 The Parties agree to take account of any guidance issued by the Information Commissioner. The Data Controllers may on not less than 30 Working Days' notice to the Data Processor amend this Data Processing Agreement to ensure that it complies with any guidance issued by the Information Commissioner.
- 3.27 The Data Controllers may, at any time on not less than 30 Working Days' notice, revise this clause by adding to it any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Agreement).
- 3.28 The Data Processor warrants and undertakes that it will deliver the Data Processing Services in accordance with all Data Protection Legislation, any Data Guidance and this Agreement and in particular that it has in place Protective Measures that are sufficient to ensure that the delivery of the Data Processing Services complies with the Data Protection Legislation and ensures that the rights of Data Subjects are protected. Processor shall not do or omit to do anything that will put the Data Controllers in breach of the Data Protection Legislation or the Data Guidance.
- 3.29 The Data Processor must assist the Data Controllers in ensuring compliance with the obligations set out at Article 32 to 36 of the GDPR and equivalent provisions implemented into Law, taking into account the nature of processing and the information available to Processor.
- 3.30 The Data Processor must take prompt and proper remedial action regarding any Data Loss Event.
- 3.31 The Data Processor must assist the Data Controllers by taking appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Data Controllers obligation to respond to requests for exercising rights granted to individuals by the Data Protection Legislation.

4 TERM AND TERMINATION

- 4.1 This Agreement shall commence on the Effective Date. Unless terminated in accordance with this clause, this Agreement shall automatically terminate on the latter of expiry or termination of the Services.
- 4.2 Without affecting any other right or remedy available to it, the Data Controllers may immediately terminate this Agreement by notice in writing to the Processor if they commit a material breach of any provision of this Agreement or the Processor repeatedly breaches any of the provisions of this Agreement.
- 4.3 On termination of this Agreement:
- 4.3.1 any rights, remedies, obligations or liabilities of the parties that have accrued up to the date of termination, including the right to claim damages in respect of any breach of this Agreement which existed at or before the date of termination, shall not be affected;
 - 4.3.2 the provisions of this Agreement which place obligations on the Data Processor in respect of the processing of pseudonymised data shall continue in force and effect until such time as all pseudonymised data (including all copies thereof) has either been returned and/or destroyed in accordance with the foregoing sub-clause (unless otherwise strictly required by Law);
 - 4.3.3 without prejudice to the foregoing sub-clause, the provisions of this Agreement that expressly or by implication are intended to come into or continue in force on or after termination of this Agreement shall remain in full force and effect; and

5 REMEDIES AND NO WAIVER

- 5.1 The limitations on liability applicable to the parties in the Services agreement shall apply to their liability under this Agreement (except in respect of express indemnification obligations under this Agreement). In addition, nothing in this Agreement excludes or limits any liability which cannot legally be excluded or limited including, but not limited to, liability for:
- 5.1.1 death or personal injury caused by negligence; and

- 5.1.2 fraud or fraudulent misrepresentation.
- 5.2 This clause 5.2 sets out specific heads of excluded loss:
 - 5.2.1 Subject to clause 5.1, the types of loss listed in clause 5.2.2 are wholly excluded by the parties.
 - 5.2.2 The Data Processor shall not be liable under this Agreement for:
 - 5.2.2.1 loss of profits;
 - 5.2.2.2 loss of sales or business;
 - 5.2.2.3 loss of agreements or contracts;
 - 5.2.2.4 loss of anticipated savings;
 - 5.2.2.5 loss of use or corruption of software, data or information;
 - 5.2.2.6 loss of or damage to goodwill;
 - 5.2.2.7 any other type of special, indirect or consequential loss.
- 5.3 The rights and remedies provided under this Agreement are in addition to, and not exclusive of, any rights or remedies provided by Law or in equity.
- 5.4 A waiver of any right or remedy under this Agreement or by Law or in equity is only effective if given in writing and signed on behalf of the party giving it and any such waiver so given shall not be deemed a waiver of any similar or subsequent breach or default.
- 5.5 A failure or delay by a party in exercising any right or remedy provided under this Agreement or by Law or in equity shall not constitute a waiver of that or any other right or remedy, nor shall it prevent or restrict any further exercise of that or any other right or remedy. No single or partial exercise of any right or remedy provided under this Agreement or by Law or in equity shall prevent or restrict the further exercise of that or any other right or remedy.

6 NOTICES

- 6.1 Any notice given to a party under or in connection with this Agreement shall be in writing in the English language and shall be sent by email to the Data Controller and Data Processor email address.
- 6.2 Any notice validly given in accordance with the foregoing clause shall be deemed to have been received the following Business Day.

7 GENERAL

- 7.1 The Processor shall not assign, transfer, mortgage, charge, subcontract, declare a trust over or deal in any other manner with any or all of its rights and obligations under this Agreement without the prior written consent of the Data Controllers.
- 7.2 No variation of this Agreement shall be effective unless it is in writing and signed by the parties to this Agreement.
- 7.3 This Agreement may be executed in any number of counterparts, each of which when executed and delivered 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 at least one counterpart.


8 GOVERNING LAW AND JURISDICTION

- 8.1 This Agreement and any dispute or claim arising out of or in connection with it or its subject matter or formation (including non-contractual disputes or claims) shall be governed by and construed in accordance with the Law of England.
- 8.2 Each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim arising out of or in connection with this Agreement or its subject matter or formation (including non-contractual disputes or claims), provided that nothing in this clause shall prevent a party from enforcing any judgement obtained in the court of England and Wales in any other court with jurisdiction over the other party.

9 SIGNATORIES

9.1 General Practice Caldicott Guardian or Senior Partner to sign here

On behalf of my General Practice, the Data Controller of primary care data, I agree to the processing of patient data for this population health management development programme in accordance with the terms and conditions outlined in this Agreement.

Signature: (Caldicott Guardian/ IG Lead or Senior Partner)	
Printed Name:	Dr Sadik Merali
Designation: (Caldicott Guardian or Senior Partner)	GP
General Practice name and address:	Ashingdon Medical Centre 57 Lascelles Gardens Rochford Essex SS4 3BW
Date:	7 th May 2021

Practice Code:	F81690
Practice Manager email (or main contact person):	Kerry Jones
Practice Manager telephone (or main contact person):	01702 533737

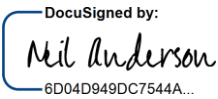
9.2 Accountable Officer, SIRO or Caldicott Guardian of NHS Basildon & Brentwood CCG, NHS Castle Point & Rochford CCG, NHS Mid Essex CCG, NHS Southend CCG and NHS Thurrock CCG to sign here:

On behalf of the CCGs, as joint data controller of the commissioning datasets (de-identified), I agree to the processing of patient data for this population health management development programme in accordance with the terms and conditions outlined in this Agreement.

Signature: Accountable Officer, SIRO or Caldicott Guardian)	
Printed Name:	Mark Barker
Job Title:	Chief Finance Officer (Senior Information Risk Officer)
Operational/main contact – email and telephone:	Monica Scrobotovici - Senior Programme Manager, Population Health Management, Mid and South Essex HCP MScrobotovici@thurrock.gov.uk 01375 652 652 x64909
Date:	19 th April 2021

9.3 SIRO or Caldicott Guardian or MD or other authorised Executive Director for Optum Health Solutions (UK) Limited, to sign here:

On behalf of Optum, the Data Processor for this population health management development programme, I agree to the processing of patient data in accordance with the terms and conditions outlined in this Agreement.

Signature: (SIRO or Caldicott Guardian or MD or other authorised Executive Director)	 DocuSigned by: Neil Anderson 6D04D949DC7544A...
Printed Name:	Neil Anderson
Job Title:	Director
Operational/main contact – email and telephone:	Dr. Marcus Green marcus.green@optum.com +44 207/479.2410
Date:	13 April 2021

Annex A

Data Specification Mid & South Essex Population Health Management

Summary	
Subject matter of the processing	<p>Population Health Management is an approach aimed at improving the health of an entire population. It is about improving the physical and mental health outcomes and wellbeing of people, whilst reducing health inequalities within and across a defined population</p> <p>It includes action to reduce the occurrence of ill-health, including addressing wider determinants of health, and requires working with communities and partner agencies.</p> <p>It improves population health by data driven planning and delivery of proactive care to achieve maximum impact</p> <p>It includes segmentation, stratification and impactability modelling to identify local 'at risk' cohorts - and, in turn, designing and targeting interventions to prevent ill-health and to improve care and support for people with ongoing health conditions and reducing unwarranted variations in outcomes.</p>
Duration of the processing	1 st June 2021 until the completion of the programme.
Nature and purpose of the processing	<p>A pseudonymised dataset, as defined below will be extracted from the practice system on behalf of the Data Controllers, using their NHS Digital approved Pseudonymisation tool. This tool removes personal patient data from each record and replaces the NHS number with a common pseudonym that can be used to link this dataset to other local and national health (primary, secondary, community) and social care datasets.</p> <p>Linked datasets created will be passed from the Mid and South Essex STP CCGs, or on behalf of the Data Controllers, on to the Processor to produce aggregate reports from this data to support the Controllers' PHM planning processes. These aggregate reports will not be identifiable and will be shared with Primary Care Networks, CCGs, and other stakeholders involved in PHM planning processes.</p>
Data Set Details	
Dataset(s)	GP Dataset
Legal Basis for Sharing	<p><i>Pseudonymised data</i></p> <p>Article 6 (1) (e) Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.</p>

	<p>In particular the responsibility of commissioners to carry out the following statutory duties under the Health and Social Care Act which will be relied upon for this programme:</p> <p>DUTY: Exercise its functions efficiently</p> <p>DUTY: Securing continuous improvement in quality of services provided to individuals</p> <p>DUTY: to promote integrated health services</p> <p>DUTY: to promote integration between health services and health-related services</p> <p>POWER: For a CCG to deliver services jointly with a combined authority</p> <p>Special Category Data</p> <p>Article 9(2)(h) Processing is necessary for the provision of health or social care or treatment or the management of health or social care systems and services.</p> <p>Article 9(2)(i) Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices</p> <p>Recital 53 Special categories of personal data which merit higher protection should be processed for health-related purposes only where necessary to achieve those purposes for the benefit of natural persons and society as a whole, in particular in the context of the management of health or social care services and systems, including processing by the management and central national health authorities of such data for the purpose of quality control, management information and the general national and local supervision of the health or social care system.</p> <p>Recital 54 The processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health without consent of the data subject. Such processing should be subject to suitable and specific measures so as to protect the rights and freedoms of natural persons. In that context, ‘public health’ should be interpreted as defined in Regulation (EC) No 1338/2008 of the European Parliament and of the Council (1), namely all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality.</p>
--	--

Compliance with confidentiality and privacy rights	<ul style="list-style-type: none"> • <u>Common Law Duty of Confidentiality and Article 8 Human Rights Act 1998</u>: The Parties will ensure they comply with these obligations by ensuring that no data that has a risk of being identified is shared without the agreement of the patient. Only pseudonymised data will be shared for population health management persons with measures to effectively anonymise this data in line with the ICO Anonymisation Code of Practice. • <u>Section 251 NHS Act 2006</u> – Under s.251, GPs, CCGs and relevant Controllers have authority to carry out risk stratification which is carried out in the public interest or in the exercise of official authority vested in the controller through GDPR Article 6 (1) (e).
Type of pseudonymised data	<p>Pseudonymised data collected will be:</p> <ul style="list-style-type: none"> • Health data including clinical diagnosis, treatments and outcomes (including mental health). • Demographic data. • Racial or ethnic origin.
Categories of Data Subject	Patients registered with the participating GP Practices
Data Extraction, Authorised Recipients and Data to be Shared	
Included in the data extracts	<p><u>Inclusion criteria</u></p> <ul style="list-style-type: none"> • Current, former and deceased patients. <p><u>Demographics</u></p> <ul style="list-style-type: none"> • NHS Number. • Date of birth. • Registered Practice <p><u>Read Coded Data (including data, code, values)</u> – Data will be extracted on the following areas; the specific Read codes searched for are modified on a frequent basis as national and local guidance changes. The current areas include:</p> <ul style="list-style-type: none"> • Flu (Vaccinations, related diagnosis, CI/allergies, refusals, carers etc.) • Prevalence – all relevant clinical diagnosis data including QOF areas. • Health Checks – nationally and locally defined HC criteria. • Admissions – all relevant clinical diagnosis data including QOF areas. • COPD. • AF. • Admission Risk. • Fracture risk. • End of Life. • Diabetes. • Heart Failure. • LD (to include details on screening, health checks, action plans, smoking, alcohol, BMI, CHD and other conditions e.g. Autism, Asthma, Dysphagia, Dementia etc.)

	<ul style="list-style-type: none"> • Frailty. • Diagnostic Testing. • Screening programmes. • Family History. • Referrals. <p><u>Outputs</u></p> <ul style="list-style-type: none"> • Events Journal (all read codes and dates relating to events activity, diagnosis etc.) • Prescription Journal (Recorded prescriptions on the patient record). • Demographics Table (combined list of patients described above).
Excluded from data extractions	<ul style="list-style-type: none"> • Any patient record with an active dissent code. • All sensitive coded data. • NHS number and date of birth are not extracted for the patients with an active refusal to consent to share coded information within their record. • No data will be extracted on patients with an active code which marks their records as being confidential.
Frequency of extraction	One off extraction
Data to be shared	<p><i>Pseudonymised Data</i></p> <p>Data will be extracted by the Mid and South Essex STP CCGs, or on behalf of the Data Controllers, from the Controllers' systems which will be pseudonymised and de-identified upon receipt in AGEM CSU (on behalf of the General Practices), for the purpose of linking with other local and national health and social care data. These linked datasets will be further shared with the Processor and to allow further PHM analyses to be carried out.</p> <p><i>Non-Identifiable Data</i></p> <p>Non-identifiable aggregate data will be generated by the Mid and South Essex STP CCGs, or on behalf of the Data Controllers, and the Processor to create reports to be shared with the Primary Care Network and partner organisations involved in the PHM process to allow informed decisions to be made on appropriate service improvements in the future.</p> <p><i>Patient Identifiable</i></p> <p>Where the population health management process has identified a particular cohort of patients where intervention is required, details will be passed to the practice to offer the appropriate intervention i.e. for direct care purposes.</p> <p>The date of birth and postcode will not be shared and will only be used to derive other data items such as a patient's age or ward in which they live. No identifiable data such as</p>

	NHS number or patient name and address will be extracted as part of this dataset.
Authorised Recipients	<ul style="list-style-type: none"> • Pseudonymised data will be shared the Mid and South Essex STP CCGs, or on behalf of the Data Controllers for data linkage purposes. Once linked to other health and social care data sources, this linked dataset will be shared with the Processor to allow analysis of this linked data set to support PHM planning. • Anonymised data in the form of aggregated reports will be shared with the Data Controllers involved in the PHM process to support the management of the health and needs of their population. • The registered GP practice of the patient will receive personal details of the patient (where patients identified as needing further intervention from the linked dataset analysis).
Special Conditions	None
Data Retention	Personal Data will be retained by Optum for the term of this Agreement plus any additional retention period required by Data Protection Legislation and in conjunction with the NHS Information Governance Alliance Records Management Code of Practice.
Annex Details	
Data Controllers Data Protection Officer	<p>Jane Marley Head of Information Governance and Data Protection Officer Mid, South and West Essex CCGs and GP Practices Phoenix Court, Christopher Martin Road, Basildon, Essex, SS14 3HG Jane.marley@nhs.net</p>
Data Processor Data Protection Officer	<p>Deanna Dicarantonio Data Protection Officer, VP International Privacy Program and Innovation, UnitedHealth Group uhg_privacy_office@uhc.com</p>

Annex B

Additional Data Processor Instruction to Arden & GEM CSU

The Data Controllers instruct Arden and Gem to flow data to Optum Health Solutions (UK) Ltd, as per the 4 spreadsheet specifications which have been embedded below.

The data sets that will flow are SUS: APC (Inpatients); NAC (Outpatients); AE (Accident & Emergency)



Optum Acute Data
Spec - 2021-01-26 v2

The data collected will be within the time period: April 2017 to date, this will be a one-off data flow.

GP Data:



Optum General
Practice Data Spec -

Data collected will be for the time period detailed within document, this will be a one-off data flow.

Community health, and Mental Health data: Patient; Activity; Diagnosis



Optum Community
and MH Data Spec -

Data collected will be within the time period: April 2017 to date, this will be a one-off data flow.

Waiting list data: Provider; Specialty; Pathway



Optum Waiting List
Data Spec - 2020-06

Data collected will be within the time period: April 2020 to date, this will be a one-off data flow.

In addition to the above, should the national Adult Social Care commissioning dataset become available during this programme, the output of this dataset will also be provided.

Data collected will be within the time period: April 2017 to date, this will be a one-off data flow.

The signature of the Arden and GEM CSU SIRO below confirms the CSU's acceptance of the instruction to provide the specified data to Optum Health Solutions as per this Annex.

Signature:	
Printed Name:	
Job Title:	
Date:	