Nottingham and Nottinghamshire
Clinical Commissioning Group

Data Processing Agreement

BETWEEN

…….Practice

(Hereinafter also known as the Data Controller)

AND

NHS Nottingham and Nottinghamshire Clinical Commissioning Group

(Hereinafter also known as the Data Processor)

In Support of the Provision of a Medicines Optimisation Service for General Practice

THIS AGREEMENT IS MADE ON THE ……..

1.0 Background Information

1.1 The service Data Processor is **NHS Nottingham and Nottinghamshire Clinical Commissioning Group (CCG)** which provides a Medicines Optimisation Service **to GP Practices** . The service includes support and facilitation for functions connected with ensuring effective medicines optimisation within the practice/s.

1.2 This Agreement provides an operating framework to enable lawful disclosure of Data to the Data Processor working on behalf of the Data Controller taking account of the Data Protection Legislation, the Common Law Duty of Confidentiality, and other applicable legislation.

1.3 The terms and conditions of this Agreement shall apply to all Data provided by the Data Controller, or provided to the Data Processor on behalf of the Data Controller, or obtained by the Data Processor from other sources as part of the delivery of the contracted services, or derived from any combination thereof.

1.4 This Agreement between the Data Controller and the Data Processor supports all **Data processed by the Data Processor of behalf of the Data Controller** in relation to Medicines Optimisation. This includes storing; transforming; deriving; analysing and making reports available to the Data Controller, at either identifiable level (personal data) or aggregate level as required, along with the provision of aggregated level reports to NHS Nottingham and Nottinghamshire CCG on behalf of the Data Controller. It will further support any additional data processing activities agreed with the Data Controller through a Service Level, or equivalent agreement.

2.0 Definitions and Interpretation

The following definitions shall apply in this agreement.

2.1 **Aggregate Data –** As per the Information Commissioner Office website, aggregate data is statistical data about several individuals that has been combined to show general trends or values without identifying individuals within the data.

2.2 **Data Protection Legislation** means (i) the DPA 1998 (ii) the GDPR, the LED and any applicable national Laws implementing them as amended from time to time (iii) the DPA 2018 (iv) 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

2.3 **Data –** any information as defined in 2.1, 2.12, 2.13 and 2.14 that the Data Controller is responsible for exercising control of. This includes all information supplied to the Data Processor by the Data Controller, or provided to the Data Processor on behalf of the Data Controller and any additional information that the Data Processor obtains during the term of the contract and shall apply equally to original Data and all back-up and/or copies printed out.

2.4 **Data Controller –** Shall take the meaning as defined in the Data Protection Legislation

2.5 **Data Processor –** Shall take the meaning as defined in the Data Protection Legislation

2.6 **Data Processing –** Shall take the meaning as defined in the Data Protection Legislation

2.7 **Data Protection Impact Assessment (DPIA) -** is an assessment carried out by the Data Controller to identify the impact of any processing of personal data.

2.8 **Data Protection Officer (DPO)** - Shall take the meaning given in the Data Protection Legislation.

2.9 **GDPR** – General Data Protection Regulation 2016

2.10 **Information Commissioner**'s **Office** - Upholds information rights in the public interest, promoting openness by public bodies and data privacy for individuals.

2.11 **LED** – Law Enforcement Directive (Directive (EU) 2016/680)

2.12 **Other Confidential Information -** any information or combination of information that contains details about an organisation or an individual person that was provided in an expectation of confidence. This includes for example, non-personal corporate or technical information that is commercially sensitive, drafts of documents that are not ready for publication, restricted information and documents, etc. as well as personal data about patients, service users and staff, including deceased individuals.

2.13 **Personal Data –** Shall take the meaning as defined in the Data Protection Legislation.

2.14 **Pseudonymised Data** – Shall take the meaning as defined in the Data Protection Legislation.

2.15 **Recipient** - any person to whom the data are disclosed, including any person (such as an employee or agent of the data controller, a data processor or an employee or agent of a data processor) to whom they are disclosed in the course of processing the data for the data controller, but does not include any person to whom disclosure is or may be made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law**.**

2.16 **Sub- Processor** – means any third party appointed to process Personal Data on behalf of the Data Processor related to the agreement.

3.0 Description of Data/Reports

3.1 The Data covered in this Agreement is as detailed in section 3.2 and where relevant is indicated as aggregate data, other confidential information, personal data and pseudonymised level data (as defined in paragraphs 2.1, 2.12, 2.13 and 2.14 respectively). The Data Processor shall not disclose any Data to any third party without the prior written consent of the Data Controller, either through this Agreement or a separate written instruction from the Data Controller.

The Data Processor will undertake work in primary care to deliver improvements in safe, cost effective evidence based prescribing of medicines and medical devices on behalf of, and in agreement with practices. This may require the processer to extract data within one practice or across a number of practices at the same time as a single data extraction search eg a data search across a federated group.

3.2 Requirements

3.2.1 Type of personal data: Name, address, date of birth

3.2.2 Special categories of personal data; race, ethnic origin and health

3.2.3 Categories of data subject: staff, patients, patients carers, third party providers (e.g. community pharmacy, dieticians)

3.2.4 Patient's Confidential Data (PCD) will be processed in support of the Data Processor's Service to provide advice on medicines optimisation and prescribing queries, and review prescribing medicines to ensure it is safe and cost-effective.

The Data Processor will process patients' confidential data (PCD) as follows (this list is not exhaustive)

3.2.5 SystmOne or EMIS Web searches for patients with potential causes of medicines-related harm, followed by review of the records of patients whose prescriptions put them at risk of significant harm, to enable a suitable suggestion to reduce the clinical risk to be made to the Data Controller.

3.2.6 SystmOne or EMIS Web searches for patients who are prescribed a specific drug, followed by viewing these patients' records to check they have no contra-indication or other obvious reason not to switch to a lower cost drug that is as effective or more effective.

3.2.7 When checking that a patient has no contra-indication to a lower cost drug finds another aspect of the prescription that merits investigation (e.g. a safety risk).

3.2.8 When performing training and induction of staff, trainee will view work outlined above to reduce medicines-related harm or avoid unnecessary expenditure, or during peer review of a Medicines Optimisation Team (MOT) undertaking this work.

3.2.9 During the preparation and refinement of the work outlined above to reduce medicines-related harm or avoid unnecessary expenditure, to ensure the work is safe and effective.

3.2.10 SystmOne or EMIS Web searches for patients whose polypharmacy may be problematic (e.g. they are prescribed at least 10 medicines and have at least one potential cause of significant medicines-related harm). The MOT member reviews the notes of patients found by the search:

- to establish if there is any obvious reason not to invite them to the practice for a medication review
- who have already accepted an invitation to a medication review.

3.2.11 When a GP has asked their MOT member to review a specific patient's record, usually when the GP has a question about the patient's drug treatment or undertake a general medication review.

3.2.12 When another member of the practice team (e.g. a practice nurse, practice manager, clinically embedded pharmacist or health care assistant) has requested advice from a MOT member on a prescription- or medicines-related aspect of the patient's care.

3.2.13 To support the delivery of waste medication reduction e.g. review and removal of repeat templates. Altering and aligning of medication quantities.

3.2.14 In connection with provision of funding to hospitals for high cost medicines that are not included in national tariff prices:

- Patients' hospital and NHS numbers are provided on funding requests. These are used by MOT member and a database coordinator to check that the patient is registered at a general practice (so that CCG is responsible for funding the medicine for the patient).

- Patients' hospital numbers are provided on the spreadsheet (SLAM) that MOT member and the database coordinator use to check that hospitals are only charging us for medicines following approval by the CCG of a funding request for the medicine for that patient.

3.2.15 When working in care homes residents medicines administration record (MAR) charts will be reviewed and checked against the patient's SystmOne or EMIS-web record if errors are suspected. Any changes will be communicated to the practice. Additional work areas may also be requested in care homes see care home pharmacist intervention agreement.

3.2.16 Accessing patient records to obtain demographics in order to respond to medicines related queries.

3.2.17 Supporting the CCGs statutory requirements linked to the monitoring of Controlled Drug prescribing.

3.2.18 Other examples may include FP10 prescription recall from NHSBSA- e.g. for CD monitoring, prescribing code issues or other issues.

4.0 Data Controller Responsibilities

4.1 The Data Controller is the Data Controller of the data insofar as it is personal data as defined by Data Protection Legislation and, shall at all times, ensure that personal data is only processed lawfully and in accordance with the Data Protection Legislation.

4.2 It is the legal duty of the Data Controller to comply with the Data Protection Legislation in relation to all personal data with respect to which he is a Data Controller (unless an exemption applies).

4.3 The Data Controller shall not instruct the Data Processor to process personal data on its behalf under this agreement where the Data Controller itself does not have a secure basis in law to process that data.

4.4 The Data Controller is legally responsible for the data processing carried out by the contracted Data Processor.

4.5 Under the terms of this agreement the Data Controller shall provide the Data processor with the minimum amount of Data necessary to deliver the contracted service. In the case where data is received by the Data Processor on behalf of the Data Controller from another source, only the minimum amount of Data will be processed to meet the objective.

4.6 The Data Controller will ensure that it authorises and documents specific data types and access levels for individual Data Processor Recipients .

4. 7 In controlling access to the Data the Data Controller will ensure that appropriate Smartcard permissions are in place.

4.8 The Data Controller will ensure that it monitors and audits Data Recipient access to its systems.

4.9 The Data Controller will not contract services from Data Processors unable or unwilling to comply with the terms of this Agreement and reserves the right to terminate the contract if either party is unable to agree necessary amendments in future.

4.10 The Data Controller will supply the Data Processor with documentation as outlined in 13.2.1

5.0 Data Processor Responsibilities

5.1 NHS Nottingham and Nottinghamshire CCG Medicines Optimisation Team, is the Data Processor and shall at all times only process the personal data in its possession and held on behalf of the Data Controller lawfully and as instructed by the Data Controller and in accordance with Data Protection Legislation and this agreement. If the Data Processor is required to do otherwise by law the Processor will notify the Data Controller promptly before processing the Personal Data unless prohibited by Law.

5.2 The Data Processor undertakes to fully comply with all related and relevant legislation, regulatory and industry standards, including (but not limited to) Data Protection Legislation as defined in this agreement; the Human Rights Act 1998; the Common Law Duty of Confidentiality; the Computer Misuse Act 1998, the NHS Care Record Guarantee, the NHS Constitution, the NHS Code of Confidentiality; Caldicott Principles and guidance issued by the Information Commissioner as the Regulatory Body and NHS England.

5.3 The Data Processor will inform the Data Controller immediately if it is asked to undertake any processing that would infringe the Data Protection Legislation of the EU or any member state.

5.4 Where relevant, the Data Processor shall comply with the Data Controller's obligations contained in any contract or agreement the Data Controller enters into with NHS Digital (HSCIC) such as a Data Sharing Framework Contract or any specific Data Sharing Agreement, or any other similar obligations of the Data Controller as notified to the data processor by the Data Controller.

5.5 The Data Processor shall not cause or allow Data to be transferred to any territory outside the European Economic Area without the prior written permission of the Data Controller.

5.6 Any unauthorised processing by the Data Processor of the Data Controller's personal data beyond the terms and conditions set out in the agreement is unlawful and will be dealt with by the Data Controller as a personal data breach in accordance with NHS policy (See Section 7).

5.7 The Data Processor shall put in place appropriate technical and organisational measures against any lawful processing of Data and against accidental loss, destruction of and damage to Data; such measures will be commensurate with the category of data being processed (as per 2.1, 2.12, 2.13 and 2.14).

5.8 The Data Processor shall ensure that the data for which the Data Controller is responsible shall be held securely and separately from any other data that the Data Processor is required to hold under contract with other persons.

5.9 The Data Processor shall provide reasonable cooperation and assistance in relation to the provision of the necessary assurances and guarantees, to the Data Controller in their responsibility to ensure compliance with the technical and organisational security measures to protect the processing of personal data.

5.10 The Data Processor agrees to maintain good information governance standards and practices, and, as a minimum, will meet or exceed the Data Security & Protection Toolkit requirements specified in section GC21 of the General Conditions of the NHS Contract, or to an equivalent standard in any subsequent NHS Information Governance compliance tool/process.

5.11 The Data Processor shall have confidentiality, information security, data protection and records management policies as required by the NHS Information Governance toolkit (or to any subsequent replacement Information Governance compliance tool/process)

5.12 The Data Processor shall have appropriate procedural/guidance documents which outline the processing undertaken by the data processor's staff that will demonstrate compliance with this agreement.

5.13 The Data Processor shall provide the Data Controller with copies of policies & procedures referred to in 5.11 and 5.12 above.

5.14 The Data Processor agrees to attain the standards of information governance practice that the Data Controller is required to attain.

5.15 The Data Processor shall assist the Data Controller and provide any necessary information for the completion of Data Protection Impact Assessments. (DPIA)

5.16 The Data Processor shall provide reasonable assistance to the Data Controller where the outcome of a DPIA necessitates consultation with the Information Commissioner's Office.

5.17 The Data Processor will designate a Data Protection Officer and will communicate to the Data Controller the name and contact details of any Data Protection Officer.

6.0 Confidential Personal Data

6.1 The Data Processor shall not store, copy, disclose or use the Data Controller's data except as necessary for the performance by the Data Processor of its obligations under this Contract or as otherwise expressly authorised in writing by the Data Controller.

6.2 In particular, the Data Processor shall not share the personal data that the Data Controller is responsible for with any, individual, business or third party (in whole or in part) without the prior agreement and written permission of the Data Controller; nor process personal data in any way or for any purpose that has not been instructed and authorised by the Data Controller.

6.3 The Data Processor shall not subcontract any of its processing operations performed on behalf of the Data Controller under this Agreement (with the exception of IT services including data destruction of electronic or hard copy Data) without the prior written consent of the Data Controller. Where the Data Processor subcontracts its obligations, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data processor under this Agreement. Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data processor shall remain fully liable to the Data Controller for the performance of the sub-processor's obligations under such agreement.

6.4 For the avoidance of doubt, a third party in the context of this agreement is any person other than the Data Controller and its staff or the Data Processor and its staff authorised to process data on behalf of the Data Controller.

6.5 The Data Processor shall not delete or remove or otherwise dispose of any personal data or information that the Data Controller is responsible for without the express authorisation of the Data Controller.

6.6 The Data Processor will keep a record of all processing of personal data it carries out on behalf of the Data Controller.

7.0 Data Security Requirement

The Data Processor shall:

7.1 Put in place appropriate technical and organisational measures to ensure the protection of the Data which is subject to this Agreement against the accidental loss or destruction of or damage to Data, having regard to the specific requirements set out in this Agreement, the state of technical development and the level of harm that may be suffered by the Data Controller and/or by a Data Subject whose Personal data is affected, by such unauthorised or unlawful processing or by its loss, damage or destruction.

7.2 Take reasonable steps to ensure the reliability of the Data Processors' personnel who have access to the personal data, which shall include:

7.2.1 Ensuring that all staff engaged by the Data Processor, including agency and contract staff, required to access the Data Controller's data understand the confidential nature of the personal data, and have received appropriate training to understand and comply with their responsibilities under Data Protection Legislation, the Common Law duty of Confidentiality and this agreement prior to their use of the data. The Data Processor will provide the Data Controller with evidence of that training on request.

7.2.2 The Data Processor shall include appropriate confidentiality clauses in employment contracts, including details of sanctions against employees acting in a deliberate or reckless manner that breaches confidentiality or the non-disclosure provisions of the Data Protection legislation or causes damage or loss of data

7.2.3 Have a documented disciplinary policy and procedure that clearly states the action that will be taken in the event of a Data breach.

7.2.4 Undertaking all reasonable background checks to ensure the reliability of all employees who are likely to use or have access to the Data.

7.2.5 The Data Processor shall ensure that all employees are aware of and act in accordance with policies and procedures referred to in 5.11 and 5.12.

7.3 In controlling access to the Data Controller's Data ensure:-

7.3.1 That access to the personal data is on a strict 'need to know basis' and is limited to only those employees who need access to meet the Data Processor's obligations as instructed under this agreement;

7.3.2 That it has properly configured and documented access rights for its staff, including a well-defined starters and leavers process to ensure appropriate access control;

7.3.3 That suitable and effective authentication processes are established and used to protect personal data;

7.3.4 That Recipients access specific data types and at the level defined and agreed with the Data Controller.

7.3.5 That audit and monitoring systems are in place to monitor access to the Data Controller's personal data and to ensure such access is appropriate and authorised and staff comply with organisational policy and the law;

7.3.6 That appropriate disciplinary action will be taken against any unauthorised access, unlawful disclosure or misuse of the personal data. Any personal

data breach incident should be reported to the Data Controller in accordance with Section 11.

7.3.7 That any staff involved in delivery of the contracted service who do not specifically need to use personal information as part of their role have access restricted to anonymised data, pseudonymised data and/or redacted extracts only.

7.4 Employees must not access the Data Controller's data remotely e.g. from home or via their own electronic device or internet portal other than through a secure electronic network, when authorised to do so and in accordance with organisational remote working policy.

7.5 Employees must not hold the Data Controller's data on personal equipment and, where it is essential to hold data on approved NHS portable devices; it is authorised and held securely in accordance with NHS policy;

7.6 Where data is transferred it must be transferred securely, only where it is essential to do so in relation to this agreement and when data is transferred electronically it is encrypted to the higher of the international data encryption standards for healthcare and National Standards (this includes data transferred over wireless or wired networks, held on laptops, CDs, memory sticks and tapes).

7.7 Where instructed by the Data Controller to dispose data, it is disposed of securely and confidentially in accordance with Section 13.

8.0 Security – IT Systems

8.1 The Data Processor shall hold electronically-based Data on secure servers in accordance with NHS information security standards.

8.2 Data will, under no circumstances, be stored on unencrypted portable media or devices such as laptops or USB memory sticks or CD-ROM.

8.3 The Data Processor shall ensure that all portable media used for storage or transit of Data is fully encrypted in accordance with current NHS Guidelines on encryption.

8.4 The Data Processor shall not allow employees to process Data on their own personal computers.

8.5 The Data Processor shall ensure adequate back-up facilities to minimise the risk of loss of or damage to Data and that a robust business continuity plan is in place in the event of restriction of service for any reason.

8.6 The Data Processor shall not transmit personal Data by email except where encrypted to 256 bit AES\Blowfish standards or from NHS mail to NHS mail.

8.7 The Data Processor shall ensure that any other method of data transmission is in accordance with the NHS Information Security Assurance Detailed Guidance on Secure Transfers of information available from the NHS Digital (HSCIC) website, for example, secure file transfer protocol.

8.8 The Data Processor shall ensure that any data management environment hosted by the Data Processor will be secure and in compliance with NHS information security standards; that only authorised staff of Data Processor will be granted access to Data and that such access will be to the minimum amount of data necessary. The Data Processor shall undertake only to grant access to any other users who are not staff of the data processor, upon the authorisation of the Data Controller.

8.9 The Data Processor shall only make printed paper copies of Data if this is essential for delivery of the contracted service.

9.0 Security - Physical

9.1 The Data Processor shall ensure that all Data is physically protected from accidental or deliberate loss or destruction arising from environmental hazards such as fire or flood.

9.2 The Data Processor shall ensure that all Data is held on premises that are adequately protected from unauthorised entry and/or theft of Data or any IT equipment on which it is held by, for example, the use of burglar alarms, security doors, ram-proof pillars, controlled access systems, etc.

10.0 Business Continuity

10.1 The Data Processor shall ensure it has documented Business Continuity Plans (BCP) in place which are reviewed, kept up to date and tested for of all of the Data Controller's critical information assets. The BCP shall detail the processes and arrangements which the Data Processor will follow to ensure continuity of the business processes and operations supported by the Data Processor following any failure or disruption or element of the services and recovery of those services in the event of a disaster.

10.2 The BCP will set out the various possible levels of failures of or disruptions to the service and the services to be provided and the steps to be taken to remedy the different levels of failure and disruption and the conditions or circumstances under which the Major Incident Plan is invoked.

11.0 Incident Reporting & Duty of Candour

11.1 The Data Processor shall have procedures in place to monitor access and to identify unauthorised and unlawful access and use of personal data.

11.2 The Data Processor shall immediately notify the Data Controller of any untoward incidents or activities that suggest non-compliance with any of the terms of the Agreement. This includes any suspected breach of confidentiality or any other information governance or cyber security incident. This includes 'near miss' situations even if no actual damage to or loss or inappropriate disclosure of Data results.

11.3 The Data Processor will co-operate fully with the Data Controller into the investigation of any activity outlined in 11.2 above. Any such investigation must be consistent with the current national requirements for incident reporting. At the time of writing this Agreement the current requirements are contained in the HSCIC (NHS Digital) document "Checklist Guidance for Reporting, Managing and Investigating Information Governance and Cyber Serious Incidents Requiring Investigation".

11.4 In so far as the Data Controller is responsible for the personal data, it is the Data Controller's responsibility to ensure that the incident is reported in accordance with the Department of Health policy and procedures are in place for informing data subjects as appropriate.

11.5 The Data Processor will provide assistance as requested by the Data Controller in relation to informing Data Subjects about any incidents, including communication with the Data Subject

12.0 Requests for Information & Complaints

12.1 The Data Processor shall notify the Data Controller immediately if it receives:

12.1.1 A request from a Data Subject to have access to that person's personal data; or

12.1.2 A request to rectify, block or erase any personal data; or

12.1.3 A request for information under the Freedom of Information Act 2000 (FOIA); or

12.1.4 Any communication from the Information Commissioner connected with the personal data processed under this agreement; or

12.1.5 A complaint or request relating to the Data Processor and/or the Data Controller's obligations under Data Protection Legislation, in relation to the Data being processed by the Data Processor.

12.2 The Data Processor will provide full cooperation and assistance to the Data Controller in relation to any request or complaint or request, and will:

12.2.1 Provide the Data Controller with full details of the request or complaint;

12.2.2 Comply with the data access request with the relevant timescales set out in the legislation

12.2.3 Only act upon the specific instructions of the Data Controller in relation to any such request.

13.0 Data Retention & Secure Destruction

13.1 All Data (see 3.2) above remains the property of the Data Controller and shall be either returned or destroyed by the Data Processor after an agreed period after completion of the contracted service, in a manner agreed with the Data Controller.

13.2 NHS data is subject to legal retention periods and should not be destroyed unless the Data Processor has received specific instruction to do so from the Data Controller. Where data has been identified for disposal:

13.2.1 The Data Processor shall retain personal data/reports in line with the Data Controller's records retention schedule.

13.2.2 Aggregate level data/reports shall be retained for a period of 6 years enable trend analysis reporting.

13.2.3 The Data Processor shall ensure that NHS information held in paper form (regardless of whether originally provided by the Data Controller or printed from the Data Processor's IT systems) is destroyed using a cross cut shredder or subcontracted to a confidential waste company that complies with European Standard EN15713.

13.2.4 The Data Processor shall ensure that electronic storage media used to hold or process NHS Information is destroyed or overwritten to current CESG standards as defined at www.cesg.gov.uk

13.2.5 In the event of any bad or unusable sectors that cannot be overwritten, the Data Processor shall ensure complete and irretrievable destruction of the media itself.

13.2.6 The Data Processor shall provide the Data Controller with copies of all relevant overwriting verification reports and/or certificates of secure destruction of NHS information at the conclusion of the contract.

13.2.7 Where the Data Processor engages the services of a 3rd Party data Destruction Company (for electronic or hard copy Data) the Data Processor will ensure that the standards required in 13.2.1 are complied with and that prior written consent is obtained from the Data Controller.

14.0 Monitoring & Audit

14.1 The Data Processor shall permit the Data Controller to monitor compliance with the terms of this Agreement, by:

14.1.1 Allowing Data Controller employees or nominated representatives to enter any premises where Data is held, at all reasonable times and with or without prior notice, for the purpose of inspection.

14.1.2 Completing and returning a Data Processing Monitoring Form at the request of the Data Controller.

14.1.3 Undertaking an annual independent audit of its Data Security and Protection Toolkit audit to provide assurance that the self-assessment is accurate and a true indication of performance against the prescribed standards and, shall provide the Data Controller with a copy of the report if requested to provide assurance that the contracted requirement is fully met.

15.0 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.

16.0 Agreement Duration & Effect

16.1 The Data Controller may terminate this Agreement with immediate effect by written notice to the Data Processor on or at any time after the occurrence of an event that gives rise to an information security incident or otherwise poses a risk of non-compliance with the data protection principles or this Agreement.

16.2 This Agreement will remain in force for as long as the Data Processor is commissioned to provide the Service requiring data processing as per 3.2, unless it is superseded by a newer version. A newer version may be initiated for a variety of reasons e.g. change in terms and conditions/role and responsibilities mutually agreed between both Parties.

16.3 Any minor changes to this Agreement that may become necessary from time to time shall be made by the Data Controller to the Data Processor, or requested by the Data Processor from the Data Controller, as a written variation.

16.4 In the event of major changes being required, the Data Controller shall terminate this Agreement and replace in full with an updated version. Such termination and replacement may also be initiated by the Data Processor, subject to prior arrangement with the Data Controller.

16.5 The terms of the contract will be reviewed after 3 years.

17.0 Extent of Liability

17.1 Nothing within the agreement relieves the Data Processor of its own direct responsibilities and liabilities under Data Protection legislation.

17.2 Neither Party shall be liable to the other Party for any loss or damage, costs or expenses incurred or suffered by the other Party as a result of any breach of the terms of the Agreement, unless the same were in the reasonable contemplation of the Parties at the time when they entered into the Agreement.

DATA PROCESSING AGREEMENT BETWEEN THE DATA CONTROLLER AND THE DATA PROCESSOR

On behalf of the Data Controller

The Data Controller : .....

Signed……..... Date ……

Name…….....

Position……..

(Print name & position of authorised signatory)

On behalf of the Data Processor

The Data Processor: NHS Nottingham and Nottinghamshire Clinical Commissioning Group

Signed……..……..... Date ……

Name:

Position: Chief Nurse & Director of Quality

Signed …… Date ……

Name:

Position ; Information Governance Lead- CCG