NHS
North East London
Integrated Care Board

DATA PROCESSING AGREEMENT (DPA)

Project Title: Quality Alerts

NORTH EAST LONDON ICS

Data Sharing Framework

Data Sharing Protocol (DSP)

The Data Sharing Protocol (DSP) establishes the North East London Integrated Care System framework for the sharing of Personal Data between its Members in support of Interoperability projects. It also defines the general principles, standards and procedures that each Member shall adhere to and the responsibilities that each Member owes to other Members in respect of the shared Personal Data.

Data Sharing Specification (DSS)

The Data Sharing Specification (DSS) defines the specifics of each individual interoperability project. Completed on a case-by-case basis, the DSS defines the data that will be processed, the purposes, the legal basis, the sharing type and the conditions under which the project will be executed.

Data Processing Agreement (DPA)

Data Sharing Agreement (DSA)

Depending on the specificities of each project:

- **Data Processing Agreement (DPA)**: used where a Member or a third-party organisation processes data on behalf of and under strict instructions from Members who are party to the DSS;
- **Data Sharing Agreement (DSA)**: used where a third-party organisation, alone or jointly with Members, determines the purpose and means of the processing of data in a DSS.

Configuration Management – DPA Template

Configuration Management	
Document Title:	Data Processing Agreement (DPA) Template
Authors:	Information Governance Services Ltd (IGS)
Approvers:	
Approval Date:	
Next Review:	
Version	0.1

Amendment Log		
Version	Summary of Amendments	Date
0.1	First draft by Information Governance Services Ltd (IGS)	04/07/2022

Configuration Management – DPA Content

Configuration Management	
Document Title:	Quality Alerts Data Processing Agreement
Authors:	IGS Jeanette Weismann
Approvers:	
Approval Date:	
Next Review:	
Version	0.3

Amendment Log		
Version	Summary of Amendments	Date
0.1	First Draft	30/04/2025
0.2	Second Draft	08/05/2025
0.3	Third Draft	21/05/2025

NHS
North East London
Integrated Care Board

Data Processing Agreement

This DPA is dated [----25 June---] of 2025

PARTIES

DATA CONTROLLER(S)	
Name of Organisation	**Care Setting**
NEL General Practices	Primary Care
Independent and non-NEL Providers	Secondary Care

(henceforth "Controller"); and

DATA PROCESSOR		
Name of Organisation	**ICO Registration Number**	**Address, Postcode, City and Country**
North East London Integrated Care Board (NEL ICB)	ZB387865	Unex Tower 4th Floor, 5 Station Street London United Kingdom E15 1DA

(henceforth "Processor")

each a "**Party**" and collectively the "**Parties**".

BACKGROUND

(A) The Controller and the Processor are such as defined, respectively, in paragraphs (7) and (8) of Article 4 of the UK General Data Protection Regulations (UK GDPR).

(B) The Processor has agreed to Process (as defined below) the Controller Data in accordance with Schedule 1 of this DPA, in combination with the Intellectual Property owned by the Processor, in order to provide the Services (as defined below).

(C) The Controller has agreed to allow the Processor to process the Data to carry out such Processing on the terms set out in this Processing DPA.

(D) This Data Processing Agreement seeks to clearly define the scope of the Processor's remit in processing the Personal Data and allow the Controller to discharge its duties under Data Protection Legislation.

CONTENTS

CLAUSES

SCHEDULES

1. Interpretation

1.1 In this DPA, unless the context otherwise requires, the following words have the following meaning:

Authorised Person	a director, employee, researcher, professional advisor or an agent/contractor who requires access to the Personal Data for the purpose set out in Schedule 1 of this DPA;
Authorised Representative	A named Authorised Person(s) set out in Schedule 3 who can give notice to the Processor;
Business Day	a day other than a Saturday, Sunday or public holiday in England when banks in London are open for business;
Commencement Date	shall be the DPA date set out on page 3 of this Data Processing DPA or the date Authorised Representatives of each party has signed this document. If the two dates are different, the date at which the DPA was signed shall prevail;
Confidential Information	shall be all confidential information (however recorded or preserved) disclosed by a party or its employees, officers, representatives, advisers or subcontractors involved in the provision or receipt of the Services who need to know the confidential information in question to the other party and that party's Representatives in connection with this DPA, which is either labelled as such or else which should reasonably be considered as confidential because of its nature and the manner of its disclosure.
Controller Data	shall be any information provided by the Controller for the purposes of the DPA, this is to include Personal Data and where relevant de-identified or anonymised data;
Data Processing Agreement (“DPA”)	is this agreement which sets out the terms of the processing as per Article 28 of UK GDPR;
Data Protection Legislation	laws and regulations, in any jurisdiction, that apply in relation to the Processing of Personal Data including the Data Protection Act 2018, the General Data Protection Legislation, UK GDPR and any relevant/successor legislation/regulations. It shall also include codes of practice or guidance issued by the Information Commissioner’s Office;
Intellectual Property Rights	patents, utility models, rights to inventions, copyright and neighbouring and related rights, trademarks and service marks, business names and domain names, rights in get-

	up and trade dress, goodwill and the right to sue for passing off or unfair competition, rights in designs, database rights, rights to use, and protect the confidentiality of, confidential information (including know-how and trade secrets), and all other intellectual property rights, in each case whether registered or unregistered and including all applications and rights to apply for and be granted, renewals or extensions of, and rights to claim priority from, such rights and all similar or equivalent rights or forms of protection which subsist or will subsist now or in the future in any part of the world;
'Know-How'	means any technical and other information which is not in the public domain, including information comprising or relating to concepts, discoveries, data, designs, formulae, ideas, inventions, methods, models, assays, research plans, procedures, designs for experiments and tests and results of experimentation and testing (including results of research or development), processes (including manufacturing processes, specifications and techniques), laboratory records, chemical, pharmacological, toxicological, clinical, analytical and quality control data, trial data, case report forms, data analyses, reports, manufacturing data or summaries and information contained in submissions to and information from ethical committees and regulatory authorities and computer programs or algorithms. Know-How includes documents containing Know-How, including but not limited to any rights including trade secrets, copyright, database or design rights protecting such Know-How. The fact that an item is known to the public shall not be taken to preclude the possibility that a compilation including the item, and/or a development relating to the item, is not known to the public;
Personal Data	shall have the same meaning as Section 3(2) & Section 3(3) of the Data Protection Act 2018;
Process, Processed or Processing	refers to Processing of Personal Data and shall have the same meaning as that set out in Section 3(4) of the Data Protection Act 2018;
Processed Data	means any outputs, results and/or deliverables from the processing carried out by the Processor, including but not limited to occasions where the aforementioned items might accrue Intellectual Property Rights;

Processor Data	shall be any information provided by the Processor for the purposes of the DPA, this is to include Personal Data shared by the Supplier to the Customer;
Security Breach	a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to the disclosed Personal Data;
Processor Data	shall be any information provided by the Processor for the purposes of the DPA, this is to include Personal Data shared by the Supplier to the Controller;

1.2. In this DPA, unless the context otherwise requires:

1.2.1. any phrase introduced by the terms include, including, particularly or in particular or any similar expression shall be construed as illustrative and shall not limit the sense of the words preceding those terms;

1.2.2. any reference to staff, staff member, researcher, agent, clinician, contractor or employee is describing someone who has a contractual relationship, whether corporate or unincorporated body, with the parties;

1.2.3. a reference to any statute, enactment, order, regulation or other similar instrument shall be construed as a reference to the statute, enactment, order, regulation or instrument as amended, extended or re-enacted from time to time;

1.2.4. unless otherwise specified, the singular includes the plural and the masculine includes the feminine and vice versa;

1.2.5. the headings are inserted for convenience and do not affect the construction of this DPA;

1.2.6. A reference to a company shall include any company, corporation or other body corporate, wherever and however incorporated or established;

1.2.7. a reference to clauses and Schedules are to the clauses and Schedules of this DPA and references to paragraphs are to paragraphs of the relevant Schedule.

1.3 In the case of conflict or ambiguity between any provision contained in the body of this DPA and any provision contained in the Schedules or appendices, the provision in the body of this DPA shall take precedence;

2. Scope

2.1 During the term of this DPA, the Processor is authorised by the Controller to process the Controller Data along the terms set of in this DPA.

3. The rights and obligations of the Controller

3.1 The Controller is responsible for ensuring that the processing of personal data takes place in compliance with the UK GDPR (see Article 24 UK GDPR), and all applicable legislation and data protection provisions/regulations.

3.2 The Controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

3.3 The Controller shall be responsible for, among other things, ensuring that the processing of personal data, which the Processor is instructed to perform, has a legal basis.

4. Role and obligations of the Processor

4.1 The Processor will only process the Controller Data to the extent, and in such a manner, as is instructed by the Controller and necessary for the purpose set out in Schedule 1 of this DPA.

4.2 The Processor will not process the Controller Data for any other purpose or in a way that does not comply with this DPA, the Data Protection Legislation and any mandatory policies issued by the Health Research Authority, NHS England, the Department for Health and Social Care and the Information Commissioner's Office.

4.3 The Processor must promptly notify the Controller if, in the Processor's opinion, the Controller's instruction would not comply with the Data Protection Legislation.

4.4 The Processor shall:

(a) only make copies of the Controller Data to the extent reasonably necessary for the purpose set out in Schedule 1 of this DPA (which includes, for clarity, back-up, mirroring and similar availability enhancement techniques, security, disaster recovery and testing of the Controller Data);

(b) not extract, re-utilise, use, anonymise, exploit, redistribute, re-disseminate, copy or store the Controller Data other than for the purpose set out in Schedule 1 of this DPA; and

(c) not do anything that may materially damage the reputation of the Controller.

4.5 The Processor will promptly comply with a Controller request or instructions from the Authorised Representative requiring the Processor to amend, transfer, delete or otherwise process the Personal Data, or to stop, mitigate or remedy any unauthorised processing.

5. Audit

5.1 The Controller may, at any time during the DPA, request evidence that the Processor has been complying with instructions of the Controller as to how the Controller Data should be processed.

5.2 The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in the Data Protection Legislation and this agreement and allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller.

5.3 The Processor shall be afforded sufficiently reasonable time, depending on what evidence the Controller requires, in order to comply with clauses 5.2 and 5.3. In any event, the Processor shall always be afforded at least 20 Business days in order to comply.

6. Confidentiality

6.1 The Processor and the Controller acknowledge respectively that the Controller's Confidential Information includes any Controller Data and that the Processor's Confidential Information includes any Processor Data.

6.2 The Processor shall only grant access to the Controller Data to individuals under the Processor’s authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of individuals to whom access has been granted shall be kept under periodic review.

6.3 The Processor shall at the request of the Controller demonstrate that the concerned persons under the Processor’s authority are subject to the abovementioned confidentiality.

6.4 The term Confidential Information does not include any information that:

(a) is or becomes generally available to the public (other than as a result of its disclosure by the receiving party or its Representatives in breach of this clause 6);

(b) was available to the receiving party on a non-confidential basis before disclosure by the disclosing party;

(c) was, is, or becomes, available to the receiving party on a non-confidential basis from a person who, to the receiving party's knowledge, is not bound by a confidentiality DPA with the disclosing party or otherwise prohibited from disclosing the information to the receiving party;

(d) was known to the receiving party before the information was disclosed to it by the disclosing party;

(e) the parties agree in writing is not confidential or may be disclosed; or

(f) is developed by or for the receiving party independently of the information disclosed by the disclosing party.

6.5 Each party shall keep the other party's Confidential Information confidential and shall not:

(a) process any Confidential Information other than in accordance with Schedule 1 of this DPA; or

(b) disclose any Confidential Information in whole or in part to any third party, except as expressly permitted by this clause 6.

6.6 A party may disclose Confidential Information to the extent required by law, by any governmental or other regulatory authority, or by a court or other authority of competent jurisdiction provided that, as far as it is legally permitted to do so, it gives the other party as much notice of the disclosure as possible.

6.7 Each party reserves all rights in its Confidential Information. No rights or obligations in respect of a party's Confidential Information, other than those expressly stated in this DPA, are granted to the other party, or are to be implied from this DPA.

7. Security of processing

7.1 Taking into account the state of the art, the costs 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 Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk when processing Controller Data. Depending on their relevance, these measures may include the following :

(a) pseudonymisation and encryption of personal data;

(b) the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of such technical and organisational measures.

8. Assistance to the Controller

8.1 Taking into account the nature of the processing, the Processor shall implement appropriate technical and organisational measures, insofar as this is possible, to support the Controller in the fulfilment of its obligations to respond to requests relating to the exercise of data subjects' rights laid down in Chapter III of the UK GDPR.

9. Notification of personal data breach

9.1. In case of any Personal Data breach, the Processor shall, without undue delay and in any event within 24 hours of becoming aware of it, notify the Controller of the Personal Data breach, including but not limited to instances where the Processor becomes aware of:

(a) any unauthorised or unlawful processing of any Controller Data;

(b) any loss, destruction, damage, or corruption of Controller Data; or

(c) any other Security Breach.

9.2. The Processor shall assist the Controller in notifying the Personal Data breach to the competent supervisory authority, by assisting the Controller to obtain information that may include but is not limited to:

(a) the nature of the personal data including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

(b) the likely consequences of the personal data breach;

(c) the measures taken or proposed to be taken by the Controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

10. Intellectual Property Rights

10.1 The parties acknowledge that:

(a) all Intellectual Property Rights in the Controller Data are and will remain the property of the Controller or its licensors, as the case may be;

(b) if applicable, all Intellectual Property Rights in the Processor Data are and will remain the property of the Processor or its licensors, as the case may be;

(c) the Processor shall have no rights in or to the Controller Data other than the licence to receive and Process it for the purpose set out in Schedule 1 of this DPA;

10.2 The Processor and the Controller acknowledge that reference in any element of the Controller Data and the Processor Data respectively to trade names or proprietary products, where no specific acknowledgement of such names or products is made, does not imply that such names or products may be regarded by the Processor or the Controller (as the case may be) as free for general use, outside the scope of this DPA.

10.3 The Processor hereby agrees and assigns to the Controller, and shall always assign to it, all rights (including Intellectual Property Rights) in any Processed Data under this DPA. The Processor shall sign, execute and acknowledge, at the Controller's expense, any and all documents/actions as may be necessary for the purpose of securing to Controller the rights to the Processed Data.

10.4 The Intellectual Property Rights assigned to the Controller under clause 10.3 shall be deemed to be included in the licence to use referred to in clause 10.1(c) from the date when such rights arise.

11. Warranties

11.1 The Controller warrants and represents that:

(a) it is the owner of the Intellectual Property Rights in any rights licensed or to be licensed to the Processor under clause 10.1;

(b) it has the right to license the receipt and Processing of the Controller Data for the purpose set out in Schedule 1 of this DPA;

(c) as far as it is aware, the Processing of the Controller Data under this DPA will not infringe the Intellectual Property Rights of any third party; and

(d) to the best of its knowledge the Controller Data contains nothing that is defamatory or indecent.

11.2 The Processor warrants and represents that:

(a) it is the owner of any Intellectual Property Rights licensed or to be licensed to the Controller under this DPA or it has permission to license uses of such Intellectual Property Rights;

(b) it has the necessary expertise and resources to effectively discharge its obligations under clause 7.1;

(c) it will always Process the Controller Data only in accordance with Schedule 1 of this DPA; and

(d) it shall discharge its obligations under this DPA with all due skill, care and diligence.

11.3 Exclusively for the benefit of the Controller and unless expressly stated in this DPA, all warranties, conditions and terms, whether express or implied by statute, common law or otherwise, are hereby excluded to the extent permitted by law.

12. Indemnity

12.1 The Processor shall indemnify the Controller fully and keep the Controller indemnified against all costs, regulatory fines, losses, claims, proceedings, actions, damages, legal costs, expenses and any other liabilities which the Controller suffers or for which the Processor may become liable which are caused directly or indirectly from the Processor’s breach of its obligations under this DPA.

12.2 The Processor undertakes to take out insurance, from a reputable insurance company, to cover the liabilities that may arise out the indemnity provided under clause 12.1. If required by the Controller, the Processor will produce evidence of such insurance cover to the Controller.

13. Term and termination

13.1 The DPA shall be in force for [enter period] in order for the Processor to process the Personal Data as set out in Schedule 1 of this DPA.

13.2 The Controller reserves the right, as per Data Protection Legislation, to keep the nature of the Processing under review and may, by written instructions, change the scope of the Processor's activities.

14. Use of Sub-processors

14.1 The Processor may only authorise a third party (**Sub-processor**) to process the Controller Data (whether or not in combination with the Processor Data) where the Controller has given specific prior authorisation to the Processor and that the Sub-processor is named in Schedule 2 of this DPA.

14.2 Where the Processor engages a Sub-processor to carry out specific processing activities within the scope of this DPA, the contract between the Processor and the Sub-processor shall:

(a) contain terms that are substantially the same as those set out in this DPA;

(b) terminate automatically on termination of this DPA for any reason.

14.3 A copy of the contract between the Processor and the Sub-processor, including any subsequent amendments thereto, shall, at the Controller's request, be submitted to the Controller, thereby giving the Controller the opportunity to ensure that the same data protection obligations as set out in this DPA are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the contract shall not require submission to the Controller.

14.4 The Processor shall agree a third-party beneficiary clause with the Sub-processor where, in the event of bankruptcy of the Processor, the Controller shall be a third-party beneficiary to the Sub-processor agreement and shall have the right to enforce the agreement against the Sub-processor engaged by the Processor (e.g. enabling the Controller to instruct the Sub-processor to delete or return the personal data).

15. Notice

15.1 Any notice or other communication given to a party under or in connection with this contract shall be in writing and delivered via email to the single points of contact included in Schedule 4 of this DPA.

15.2 Any notice sent in accordance with Clause 15.1 of this DPA shall be deemed to have been received:

(a) at the time and date of transmission shown on the saved sent copy kept by the sender; or

(b) where the email is sent outside business hours, at 9.00am on the first following Business Day.

15.3 This clause 15 does not apply to the service of any proceedings or other documents in any legal action or, where applicable, any arbitration or other method of dispute resolution.

16. Entire Agreement

16.1 This DPA constitutes the entire DPA between the parties and supersedes all previous discussions, correspondence, negotiations, arrangements, understandings and DPAs between them relating to any Processing of Controller Data.

16.2 The Processor acknowledges that in entering into this DPA it does not rely on, and shall have no remedies in respect of, any representation or warranty (whether made innocently or negligently) that is not set out in this DPA.

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

17. Variation

17.1. Except as expressly provided in this DPA, no variation of this DPA shall be effective unless it is in writing and signed by the parties (or their Authorised Representatives).

18. Severance

18.1 If any provision or part-provision of this DPA is or becomes invalid, illegal or unenforceable, it shall be deemed deleted, but that shall not affect the validity and enforceability of the rest of this DPA.

18.2 If any provision or part-provision of this DPA is deemed deleted under clause 18.1 the parties shall negotiate in good faith to agree a replacement provision that, to the greatest extent possible, achieves the intended commercial result of the original provision.

19. No partnership or agency

19.1 Nothing in this DPA is intended to, or shall be deemed to, establish any partnership or joint venture between any of the parties, constitute any party the agent of another party, nor authorise any party to make or enter into any commitments for or on behalf of any other party.

19.2 Each party confirms it is acting on its own behalf and not for the benefit of any other person.

20. Third-party rights

20.1 A person who is not a party to this DPA shall not have any rights under the Contracts (Rights of Third Parties) Act 1999 to enforce any term of this DPA. This does not affect any right or remedy of a third party which exists, or is available, other than in that Act.

20.2 The rights of the parties to terminate, rescind or agree any variation, waiver or settlement under this DPA are not subject to the consent of any other person.

21. Governing law

21.1. This DPA 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 and Wales.

21.2. Each party irrevocably agrees that the courts of England and Wales shall have exclusive jurisdiction to settle any dispute or claim that arises out of or in connection with this DPA or its subject matter or formation (including non-contractual disputes or claims).

This DPA has been entered into on the date stated at the beginning of this document.

Schedule 1 – Information about the processing

1. Describe the purpose of the processing: *-What is the aim of this project, why is it necessary?*

The primary objective of this project is to enable NEL General Practices to efficiently raise alerts concerning potential quality risks and issues with a diverse range of healthcare providers. While most of these alerts will be communicated directly via secure email from General Practices to the relevant providers, a smaller subset will require administrative support from the Quality & Safety Team or its successor at NEL ICB. This administration will be crucial for directing alerts to smaller, independent and non-NEL provider organisations.

2. Describe the nature of the processing: - *What processing activities will be undertaken by the data processor on behalf of the data controller(s)?*

Please take into account the broad definition of processing activities, which include any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction, pseudonymisation or anonymisation.

1. **Collection**: The NEL ICB Quality and Safety Team or its successor receives the GP's alert via NHSmail, which may contain personal data (in particular NHS Numbers, providers' name and email addresses, and alert specifics).
2. **Recording and Organisation**: The NEL ICB team records the details of the alert in a spreadsheet.
3. **Storage**: The NEL ICB team saves the GP's email and related details in a designated folder on the NEL ICB drive, hosted in Microsoft Azure cloud storage.
4. **Disclosure (Transmission)**: The NEL ICB team forwards the email to the relevant provider, including the due date for their response and copying in the GP. The provider responds by return email directly to the GP, copying in the NEL ICB team.
5. **Consultation and Use**: The NEL ICB team uses the provider's response to analyse themes and trends, which involves consulting the description of what happened provided by the GP and provider.
6. **Recording and Organising Provider's Response**: The NEL ICB team records the provider's response in a spreadsheet.
7. **Storage of Provider's Response**: The NEL ICB team saves a copy of the provider's response in the same folder as the original alert.
8. **Anonymisation**: After analysing the provider's response, the NEL ICB team produces an anonymised report every 6 months (frequency may vary).

3. List the personal data that is required: *-Provide details of each data field, and a justification for each, e.g. name, address, DoB etc.*

Data field	Justification
NHS number	To enable the provider to identify the correct patient associated with a quality alert raised by a GP in order to respond to the

	specific GP concern. NHS numbers are vital for uniquely identifying individuals within the NHS system.
Name, email address, and telephone (of GPs raising alert)	To provide the identity of the GP raising the alert to the NEL ICB team and the provider to facilitate follow-up communication and accountability.
Description of quality issues	This information provides important context for the provider to be able to respond to the GP and to address the issues raised by GPs.

4. How will the data be transferred? *-Provide details of the method of transfer, including security measures such as the use of encryption etc.*

Data will be transferred via NHSmail, which utilises **Transport Layer Security (TLS)** to secure email communications.

5. Location of the data: *-Where will the data be processed? E.g. Azure environment located in the Netherlands*

NEL ICB: The data will be processed by the NEL ICB team in the UK.
Microsoft Ltd (Microsoft Azure): The data will be stored within the NEL ICB environment which utilises Microsoft Azure data centres in the UK for cloud data storage.

6. Detail the security of the processing: *-Provide details of the technical and organisational security measures that will be in place to protect the data, e.g. encryption, access controls, physical security etc.*

In Transit:
NHSmail: NHSmail utilises **Transport Layer Security (TLS)** to secure email communications.
Microsoft Azure Data Centres: All data traffic moving between datacentres is protected using **IEEE 802.1AE MAC Security Standards**, preventing physical "man-in-the-middle" attacks.

At Rest:
NEL ICB: NEL ICB adopts various confidentiality and security measures to secure data:

- Roles-based Access Controls: Access to the data will be limited only to the administrators listed below.
- Formal Approval: To gain access, individuals must obtain formal approval from the NEL Director of Quality.
- Password protection.

Microsoft Azure: Microsoft Azure adopts various confidentiality and security measures to secure data: Managed Keys and Encryption; Physical protection; and Network protection.

7. How long is the data retained by the Processor?
The data will be retained in identifiable form by NEL ICB for 10 years. The records will be deleted from the NEL ICB folder on the drive and from nhs.net. These records will not form part of the patient record.

8. How is the data erased or decommissioned by the Processor?
Data deletion is also governed by the ***NHS Records Management Code of Practice***. The responsibility for maintaining compliance with these standards rests at the NEL ICB level. Throughout the subscription to Azure services, NEL ICB has control to access, extract, and delete their data stored in Azure services.

Schedule 2 – List of Sub-Processors

Approved Sub-Processors			
Name of Organisation	**ICO Registration Number**	**Registered Address**	**Processing Activity**
Microsoft Ltd. (Microsoft Azure)	Z6296785	Microsoft Campus Thames Valley Park Reading Berkshire RG6 1WG	Cloud based data storage

Schedule 3 – List of Authorised Persons

- Head of Quality and Safety
- Senior Quality and Safety Manager
- Contact: nelondonicb.qualityalert@nhs.net

Schedule 4 – Single Points of Contact

- Jamie Sheldrake, NEL ICB Data Protection Officer - jamie.sheldrake@nhs.net.
- Sohifa Kadir, GP Data Protection Officer – sohifa.kadir3@nhs.net.
- Jeanette Weismann, Senior Quality & Safety Manager - jeanette.weismann@nhs.net.