Imperial College Healthcare NHS Trust

NW London Digital: Statement of Data Sharing (SDS)

Title	**Statement of Data Sharing (SDS)**
Authors	**Philip Robinson, DPO Imperial College Healthcare NHS Trust** **Calum Leafe, ADPO, Imperial College Healthcare NHS Trust**
Approved by	**NW London Digital Governance Group (GG)**
Approval Date	**TBA**
Review Date	**02/11/20**
Version	**1.1**

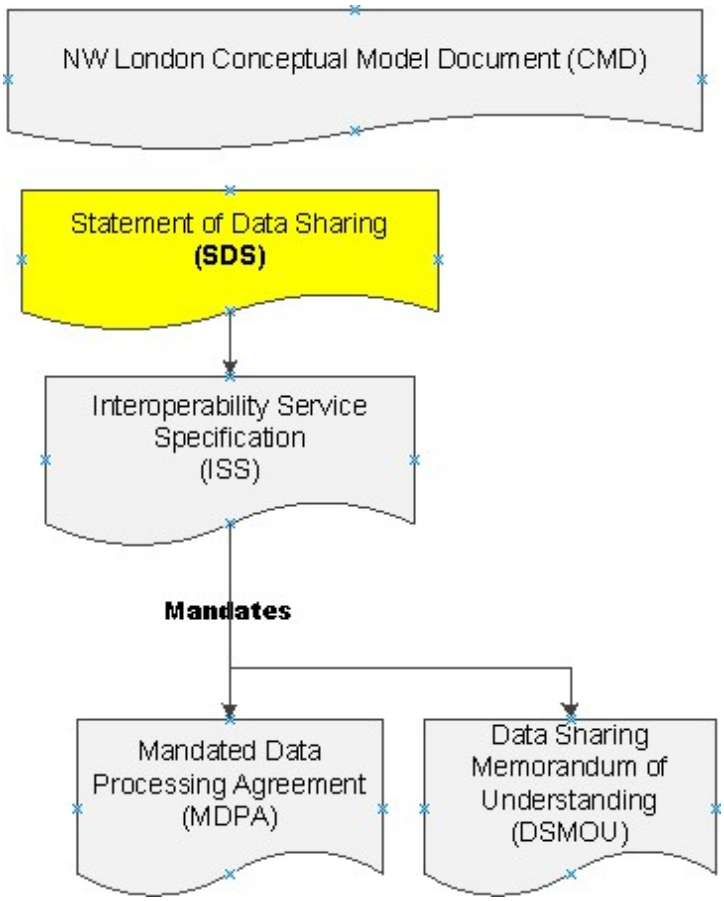
Change Log

Version	Summary of Changes	Date
0.7	Membership list removed	11/06/2019
0.6	Changes made following further legal and data protection consultancy review	06/02/2019
0.5	Version re-submitted to Capsticks LLP after changes	03/12/2018
0.4	Version Submitted to Capsticks LLP	30/11/2018
0.3	Revisions following NW London Digital Governance Group review	28/11/2018
0.2	Revisions following Caldicott Guardian and legal review	14/11/2018
0.1	First draft	10/11/2018

Distribution

Version	Distribution	Date
0.7	Primary Care	11/06/2019
0.6	NW London Digital Governance Group	
0.5	Capsticks LLP	03/12/2018
0.4	Captsicks LLP	30/11/2018
0.3	Dr Sanjay Gautama	28/11/2018
0.2	NW London Digital Governance Group	14/11/2018
0.1	Dr Sanjay Gautama; Capsticks LLP	10/11/2018

North West London Digital Data Protection Framework Diagram



Contents:

1. Introduction

1.1. This Statement of Data Sharing (SDS) is the top tier of the amended arrangements for Data sharing through the NW London Digital Data Protection Framework (DPF), set out in the NW London Digital Data Sharing Conceptual Model Document (CMD).

1.2. This Statement sets out the commitment by Members to ensuring appropriate arrangements to Data Sharing and mandates where appropriate Data Processing Agreements.

1.3. The Statement champions and promotes the sharing of data but does not provide legal indemnity to, or alter the statutory duties of, individual Controllers and Processors.

1.4. The Statement establishes the high-level data sharing relationship between the Members. The Statement covers data sharing between Members as joint or independent data controllers, but does not apply to communications between Health and Care Professionals and data subjects. It can apply to Personal Data, Special Category Data, Personal Confidential Data and non-personal data, shared in any form and by any method, including paper, recorded and electronic formats.

1.5. Organisations entering into Data Sharing and Processing Agreements referencing this Statement must only do so with the recorded explicit approval of the Governance Group and through the approved use of Interoperability Service Specifications.

1.6. All the Members have agreed to lawfully share necessary Data about their patients, service users and clients (data subjects) in support of interoperability use cases applicable as defined in each Interoperability Service Specification (ISS).

2. Membership

2.1. **Existing Members -** Signatories to the previous version of this agreement, namely the North West London Integrated Care Digital Information Sharing Agreement (Version 2) are considered to be Members to the amended NW London Digital Data Protection Framework.

2.2. **Criteria for Membership -** Membership is available to NHS organisations, NHS Trusts, General Practitioner Partnerships, general practice providers, private healthcare providers, voluntary, public and private social care providers, Clinical Commissioning Groups and and any other body subject to regulation by the Health and Social Care Act 2012.

2.3. **Geographic Restriction -** Membership is limited to organisations operating in England and notified to the Information Commissioner's Office under the terms set out in regulations made further to the Digital Economy Act 2017

2.4. **New Members Application Process -** New Members shall be subject to an application process overseen by the Governance Group via the Members Application Form. This form must be completed and signed by the applicant's

Senior Information Risk Officer (SIRO) and Caldicott Guardian, or equivalent senior representatives of organisations which do not have these roles in place. The Governance Group shall then either approve, defer subject to conditions being met, or reject, new applications, and record the outcome. On approval by the Governance Group the applicant shall be subject to the benefits and obligations of full membership.

3. Purpose of the Statement of Data Sharing

3.1. The purpose of this Statement is to facilitate the secure sharing of data amongst key public sector, private and voluntary organisations in North West London to support the provision of effective and efficient health and social care services to the populations of the local area.

3.2. The Statement sets out general principles, standards and governance agreed between the identified membership of trusted organisations to provide a secure framework for the sharing of data both as joint data controllers and individual data controllers sharing data with other individual data controllers.

4. Sharing of Personal Data

4.1. Personal data will only be shared with organisations which are able to demonstrate technical and organisational controls that demonstrate they can meet the requirements of data protection and confidentiality privacy laws, observe professional ethical standards, and protect the rights of individuals.

4.2. Personal data will only be shared lawfully, fairly and transparently for the purposes agreed under this Statement and specific Interoperability Specifications, to benefit individuals and deliver services, while protecting and respecting data subject's rights and freedoms.

4.3. Personal data shall be collected only for specified, explicit and legitimate purposes ("purpose limitation"), and only in a manner adequate, relevant and limited to what is necessary for the purpose ("data minimisaton").

4.4. Personal data may be shared where the law allows, in a manner compatible with the NHS Constitution and Caldicott Principles, and where sharing is necessary for a permitted purpose.

4.5. The Common Law Duty of Confidentiality will be respected unless: consent to disclose has been provided or can reasonably be implied; the use of the data is not a 'misuse' and/or is within the reasonable expectations of the data subject; or; there is an over-riding public interest or any other legal justification for disclosure. The parties acknowledge their duties to share information among health and social care commissioners and providers for direct care purposes where it is in the best interests of the patient, further to s. 251B of the Health and Social Care Act 2012.

5. NW London Digital Data Protection Framework

5.1. **The Governance Group (GG)** is mandated by the North West London Digital Collaboration to review, amend, and approve the arrangements for data sharing under the NW London Digital Data Protection Framework, as amended into the following components:

- Conceptual Model Document (CMD)
- Statement of Data Sharing (SDS)
- Interoperability Service Specifications (ISS)
- Mandated Data Sharing Memorandum of Understanding (DSMOU) where deemed applicable to an individual use case.

The Terms of Reference for the Governance Group are provided Appendix 1 of the Conceptual Model Document.

5.2. **Mandated Data Processing Agreements (MDPA)** - Members should ensure that they conclude and sign any mandated data processing agreements to which they are either a singular or joint party.

5.3. **Compliance** - Members are individually accountable for compliance with all legal requirements pertaining to data sharing and compliance with all requirements directly and indirectly referenced in the Statement. They are directly accountable for ensuring they are acting at all times as responsible data controllers and upholding the rights and freedoms of their respective data subjects, and they shall report any variances to compliance with this Statement to the GG.

5.4. **Compliance Requirements** - Individual members have specific obligations to ensure that they have in place robust records of processing (Article 30 GDPR), data protection impact assessments (DPIAs) (Article 35 GDPR) and the provision of appropriate transparency information and privacy notices to data subjects. (Articles 12-14 GDPR).

5.5. **Data Processors** are not Members of the NW London Digital Data Protection Framework. Instead they are directly accountable to each individual data controller who is a party to any legally binding Mandated Data Processing Agreement (MDPA) signed between the parties as a result of being mandated as a result of an ISS.

5.6. **Third Party Data Controllers** are not Members of the NW London Digital Data Protection Framework. However, a third party data controller may establish an data sharing relationship with Members under the terms of an ISS. Any new ISS must be proposed by an existing member of the statement rather than an external data controller. In addition, a mandated Data Sharing Memorandum of Understanding (DSMOU) may be concluded between Members and a third party controller.

5.7. **The Secretariat** shall provide central administration support services to the GG and are directly accountable to the dual Chairs of the GG to provide;

- Agendas
- Minutes
- Papers for review and Action
- Risk Register using a robust online risk register application available to Members at all times
- Action Log
- Decision Log
- Upload of key data to the Data Controller Console
- Update of key data to the NW London Digital Public Facing Website

5.8. **The Data Controller Console (DCC) or** an appropriate product with suitable functionality shall provide the central public repository for all relevant documents generated by the Governance Group including;

- Conceptual Model Document
- Statement of Data Sharing
- Interoperability Service Specifications
- Mandated Data Processing Agreements
- Mandated Memoranda of Understanding (ISMOU) where deemed applicable to an individual use case.

6. The Data Protection Legislation

6.1. The sharing and processing of personal data and special category data is regulated by the European Union's General Data Protection Regulation 2016, as complemented by the UK's Data Protection Act 2018 ("The Data Protection Legislation").

6.2. Members shall only share and process personal data in accordance with the principles relating to processing under Article 5 GDPR, and where a clear lawful basis is set out under Articles 6 and 9 GDPR for personal data and special category data, respectively. The members acknowledge that the typical legitimising conditions for sharing information amongst the members are:

Article 6(1) GDPR	**Article 9(2) GDPR (and Schedule 1 to the Data Protection Act 2018**
(c) The processing is necessary to comply with legal obligations	(c) The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent.
(d) The processing is necessary to protect the vital interests of the data subject or another person	(g) the processing is necessary for reasons of substantial public interest, on the basis of UK or EU law (*for instance, the discharge of statutory functions)*
(e) The 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	(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services (*in accordance with Schedule 1 paragraph 2 to the Data Protection Act 2018).*
	(i) processing is necessary for reasons of public interest in the area of public health, including ensuring high standards

	of quality and safrety of healthcare *(in accordace with Schedule 1 paragraphs 2 and 3 to the Data Protection Act 2018)*.
	(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

6.3. **The Health and Social Care Act 2012 (as amended by the Health and Social Care (Safety and Quality) Act 2015) -** Members recognise and respect the fact that compliance with s. 251B of the Health and Social Care Act 2012 (as amended by the Health and Social Care (Safety and Quality) Act 2015) creates a positive obligation for data to be shared where it facilitates care for an individual.

6.4. **Other Relevant Legislation -** Further laws and regulations by which Members are bound set out supplementary requirements around the use of personal confidential data. These include, inter alia, the NHS Act 2006, Health and Social Care Act 2012, the Human Rights Act 1998, the Common Law Duty of Confidentiality, and the EU Privacy and Electronic Communications Regulations 2003.

6.5. **Compliance with the Legislation -** The Members undertake to share and process Personal Data only where there is a clear lawful basis for doing so under Article 6 GDPR and, where concerning Special Category Data, Article 9 GDPR, and to comply with all requirements and obligations under the Data Protection legislation and all other relevant legislation.

7. Sharing and Processing Relationships

7.1. **Joint Controllership and Determination of Responsibilities -** Where two or more data controllers jointly determine the purposes and means of processing, they shall be interpreted as joint controllers under Article 26 GDPR. Joint controllers are required to determine, in a transparent manner, their respective responsibilities in the processing and sharing of data, by means of an arrangement between them.

This Statement recognises that Members may be understood to be joint controllers in individual interoperability use-cases. The Statement provides a mandate for joint controllership to be articulated and responsibilities determined in the relevant ISS for any given use-case. Where joint controllership is determined, the relevant ISS shall capture in its terms all data necessary to uphold a joint controllership arrangement in compliance with Article 26 GDPR.

7.2. **Controller to Controller** - Where two or more data controllers share data but do not jointly determine the purposes and means of its processing, they shall be interpreted as individual data controllers engaging in a controller to controller sharing relationship.

This Statement recognises that Members may be understood to be engaging in controller to controller sharing relationships. Where there is such a relationship with a Third Party Data Controller, this is to be articulated under the relevant ISS in the given use-case. The given ISS shall then provide a mandate for the conclusion of a DSMOU between the Members party to the ISS and the Third Party Data Controller.

In all instances of data controllership, Members shall be bound by the responsibilities set out under Article 24 GDPR.

7.3. **Controller to Processor** - Where processing is carried out on behalf of a controller by a third party organisation, this shall be interpreted as a controller-processor relationship.

This Statement provides a mandate for controller-processor relationships to be articulated in the relevant ISS in any given use-case. The given ISS shall then provide a mandate for the conclusion of a MDPA or MDPAs between the Members party to the ISS and the Data Processor(s).

8. Organisational Standards and Security of Processing

8.1. **Security of Processing** - All Members are obliged under Article 32 GDPR to ensure that they implement appropriate technical and organisational controls to ensure an appropriate level of security in the control and processing of data.

8.2. **ICO Registration** - Members shall ensure and maintain registration with the ICO under regulations made further to the Digital Economy Act2017, and any registration requirements under subsequent legislation.

8.3. **NHS Digital Data Security and Protection Toolkit (DSP Toolkit)** - All organisations that have access to NHS patient data and systems must provide assurance, through the DSP Toolkit, that they are practising good data security and that personal data is handled correctly.

Members shall complete the DSP Toolkit return, which shall be subject to independent audit and be designated as meeting all mandatory standards. Members shall ensure that 95% of all staff undertake annual mandatory DSP Training.

8.4. **Cyber Essentials Plus** - Cyber Essentials is a UK Government-backed certification scheme, which provides assurances that organisations are protected against a wide variety of common cyber-attacks. The ICO recognises Cyber Essentials as an appropriate ‘starting point’ for organisations’ ICT Security.

Cyber Essentials Plus certification, requiring independent assessment by a Certification Body, provides evidence of a more rigorous standard of information security protection, which allows pre-population of several criteria for the DSP Toolkit.

Members shall ensure that they are Cyber Essentials Plus certified by the end of the 2020/21 financial year, in line with the requirements set by NHS Digital.

8.5. **Staff Training** - Members shall ensure that staff receive training and guidance and abide by the rules and policies concerning the protection and use of any data covered by this Statement.

8.6. **Variance** - Any Member which is unable to comply with the stated requirements must submit a variance report to the Governance Group. The Governance Group shall take a decision whether any unmitigated risks require reporting directly to the ICO.

9. Retention Periods

9.1. **The Information Governance Alliance Records Management Code of Practice for Health and Social Care 2016** - This sets out the best practice minimum retention periods for a wide array of health and social care records. Members' organisational policies shall reflect this Code of Practice to ensure best practice in the retention of health and social care records.

9.2. **Data Decommissioning**, including the destruction, disposal, or any other management of data held by a Member, Data Processor, or Third Party Data Controller at the end of the data's lifecycle, shall be governed at the ISS level, where a detailed plan will be required.

10. Risk Management

10.1. **Data Protection Impact Assessments**

Decisions to share Personal Data will consider the impact this may have on individuals, their safety and well-being (and rights and freedoms more generally), and on others who may be affected by the decision to share.

This shall be demonstrated through the provision of an exemplar Data Protection Impact Assessment (DPIA) under each ISS. Each individual Data Controller may use the exemplar to deliver their own relevant DPIA. The management of the DPIA is entirely the responsibility of each individual Member.

The NW London Digital Governance Group Secretariat shall maintain a NW Digital Risk Log that shall comprise of strategic and operational risks for review and management by the Governance Group.

10.2. The Secretariat is responsible for maintaining a NW London Digital Data Protection Framework Risk Register (see section 5.7). The RR will be reviewed by the GG on a quarterly basis at miminum, and will be maintained on a suitable online platform available to all Members at all times.

10.3. Each individual member shall have in place their own robust approach to information risk management as mandated by the DSP Toolkit.

Each individual Member shall be responsible for attending the NW London Digital Governance Group and to review and update the RR.

11. Breach Notification and Management

11.1. **Breach Notification to the Secretariat** - Each Member shall inform the Secretariat without undue delay of any security incidents or personal data

breaches (actual or potential) pertaining to any interoperability service specification under the North West London Digital Data Protection Framework.

11.2. **Breach Management** – Any security incident or personal data breach determined by the Secretariat to present a material risk to the rights and freedoms of the data subjects concerned will be notified by the Secretariat to all Members. Such security incidents or personal data breaches shall be collated by the Secretariat and reported to the GG via Committee Papers.

11.3. **Notification to the ICO** - On advice of the Co-Chairs of the GG following informed discussion, the Secretariat may notify the ICO of any security incident or personal data breach determined to present a material risk to the rights and freedoms of the data subjects concerned.

Members as individual Data Controllers are individually accountable under the law and retain the responsibility to undertake an internal assessment as to the material impact of the security incident or personal data breach upon the rights and freedoms the data subjects to whom they are responsible. Individual organisations retain responsibility for any internal decision to notify the ICO on any subject.

12. Rights of the Data Subject

12.1. Members shall at all times discharge their responsibilities as responsible data controllers by upholding data subject rights.

Under Articles 12-22 (Chapter III) GDPR, the data subject has specific rights against any and all controllers of his/her personal data. These rights are:

i) The right to be informed
ii) The right of access
iii) The right of rectification
iv) The right of erasure (“the right to be forgotten”)
v) The right to restrict processing
vi) The right to data portability
vii) The right to object
viii) Rights related to automated decision making and profiling

The above-named rights are qualified, and not absolute rights, and should be read in line with the qualifications as set out in section 12.3 of this agreement.

The above-named rights are complemented by further rights as set out in other relevant legislative provisions including, inter alia, the right to a private family life under the Human Rights Act 1998.

12.2. Members shall use, process, and share personal data only in a manner consistent with respect for all rights of the data subject under the Data Protection legislation and any other relevant legislation.

Each Member shall have policies and procedures in place to respond to any requests by data subjects to give effect to their rights under the Data Protection legislation within a month, in the first instance.

The responsibility for the management of any requests to give effect to the rights of the data subject, including the right of rectification and the right of access to data remains with the Member as an individual organisation.

12.3. Qualifications – Certain rights under the Data Protection legislation are qualified, both generally and specifically in the health and social care context. Rights of the Data Subject, and the responsibility of the Data Controller to give effect to these rights, should be considered in line with, inter alia, the qualifications and exemptions set out in Articles 13-22 GDPR and Schedules 2-4 Data Protection Act 2018.

Requests for erasure can be refused where processing is necessary either: in the exercise of official authority vested in the controller, for health or social care purposes, or; for public health purposes in the public interest.

Members reserve the right to refuse to give effect to the rights of the data subject to the extent that any relevant qualifications or derogations apply.

13. Fair Processing and Transparency

13.1. Fair Processing and Privacy Information

Articles 12-14 GDPR set out the requirement for data controllers to provide fair processing information to the data subject about how his/her data is used. Fair processing information should be delivered through privacy notices for each category of data subject about whom data is processed or shared.

This shall be demonstrated through the provision of an exemplar privacy notice under each ISS. Any joint controllership arrangements articulated in a given ISS shall be reflected under the corresponding exemplar privacy notice.

Exemplars shall be drafted in accordance with the guidance provided by the Information Commissioner on the drafting and provision of privacy information.

13.2. Fair Processing - Obligations of the individual Member

Each individual Member shall have in place its own robust approach to the provision of fair processing information as mandated by Articles 12 - 14 GDPR.

Each individual Member shall be responsible for providing their own privacy information under each ISS and individually accountable for meeting the transparency and content requirements set out in Articles 12-14 GDPR.

Appendix 1: Procedure for Adoption of New Members

a) Proposed membership requests will have to meet the membership criteria set out in clause 2 of the SDS.

b) The membership form will be published online via the secretariat Data Protection Console that would allow proposed new members to apply and submit online;

c) All membership requests must be countersigned by the Caldicott Guardian and SIRO, or equivalent senior representatives where organisations do not have these roles in place, of the requesting organisation.

d) The submitted form will be reviewed by the secretariat and the GG Chair. If the membership request meets the criteria it will be tabled at the next available Governance Group for review / approval;

e) On approval new members will have all the benefits and responsibilities of membership.

Appendix 2: Procedure for Adoption of New Interoperability Service Specifications (ISS)

a) The ISS template form will be published online via the NW London Digital Secretariat Data Protection Console. A new ISS may only be proposed by one of the data controllers who has already adopted the Statement. (S11- changed)

b) The GG representative or Caldicott Guardian of the proposing organisation must approve the ISS before it is submitted to the secretariat.

c) The ISS template must be completed in full and be accompanied with the following supplementary documents;

- Exemplar Data Protection Impact Assessment
- Exemplar Privacy Notice
- List of Applicable Members to the ISS
- Data Flow Map
- Draft Mandated Data Processing Agreement (if applicable)
- Draft Mandated Data Sharing MOU (If applicable in limited circumstances)

d) The submitted form will be reviewed by the secretariat and the GG Chair. There will then be an opportunity for the secretariat to work with the proposer to review the template and seek and provide necessary clarifications.

e) If the ISS template form and supplementary documents meets the criteria it will be tabled at the next available Governance Group for review / approval.

Appendix 3: Procedure for Adoption of New Mandated Data Processing Agreements (MDPA)

a) The MDPA template form will be published online via the NW London Digital Secretariat Data Protection Console. The Data Protection Framework can accept either a completed MDPA template or a parallel document that covers all the requirements set out in the MDPA.

b) The MDPA is a legally binding document that all individual data controllers who are a party to the agreement with the data processor must sign off.

c) The MDPA is mandated via an approved NW London Digital ISS and therefore cannot be enacted outside an approved ISS.

d) The signed and enacted MDPA must be submitted to the secretariat by each individual party so that the final document can be stored on the Secretariat Data Protection Console and / or the Data Controller Console.

Appendix 4: Applicable Members of the NW London Digital Statement of Data Sharing

Members of NW Digital Data Protection Framework	