NHS
South West London
Health and Care Partnership

South West London Overarching Information Sharing Agreement

Current Version: 2.0 FINAL

DOCUMENT INFORMATION

Title:	South West London Overarching Information Sharing Agreement
Purpose:	This agreement, when signed, allows the sharing of specified patient information amongst the partners to this agreement.
Partners:	See appendix A
Commencement date:	**Insert date**
Review date:	**Insert date**
Agreement owner:	South West London
Version:	2.0
Status:	FINAL
Document author:	Paul Kenny, Janice Sorrell, Tanya Campbell Updated 18-Feb-2019 Sally Wiltshire for Claire Clements
Previous versions:	V1.0
Freedom of Information	

VERSION HISTORY

Version	Date issued	Updated by	Reason
V1.0	2-Sept-18	Claire Clements	Final version shared.
V2.0	19-Feb-19	Sally Wiltshire for Claire Clements	Updated DPIA inserted

TABLE OF AMENDMENTS (IF REQUIRED)

Version	Clauses Amended	Page	Summary of Amendments

Table of Contents

Abbreviations

Abbreviation	Description
DPA 2018	Data Protection Act 2018
DSP	Data Protection and Security Toolkit
EIR	Environmental Information Regulations 2004
FOIA	Freedom of Information Act 2000
GDPR	The General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.
ICO	Information Commissioner's Office
PSISA	Purpose Specific Information Sharing Agreement attached as a schedule to the South West London Integrated Care Digital Information Governance Agreement
SIRO	Senior Information Risk Owner
SWL	South West London

A glossary of data protection terminology has been provided I Appendix D at the end of this document.

INTRODUCTION

BACKGROUND

This agreement provides an overarching framework for information sharing between partner organisations in South West London (SWL). SWL is a collaborative approach between the Health and Social Care organisations across the London Boroughs of Croydon, Richmond, Merton, Sutton, Wandsworth and the Royal Borough of Kingston upon Thames.

This agreement ensures that people's information is stored and used legally and in line with national standards.

People will be able to opt out of sharing their data through the agreed SWL opt out process, however doing so may affect the care and services they would be able to access.. It is noted that the SWL opt out process is separate to and not connected with the National Data Opt-Out.

CHANGES TO DATA PROTECTION LAW

On the 25 May 2018 the 1998 Data Protection Act was replaced by the European General Data Protection Regulation 2016 and a new UK Data Protection Act.[1]

As the UK is still a member of the European Union as at 25 May 2018, the GPDR will come into full effect regardless of ongoing Brexit negotiations. This information sharing agreement takes into account compliance with the new regulation and follows current best practice guidance as set out in the UK Information Commissioner's "Data Sharing Code of Practice".[2] This Agreement should be reviewed once the UK Data Protection Act 2018 has been published.

[1] (EU) 2016/679 General Data Protection Regulation. The UK Data Protection Bill is currently passing through parliament. Once enacted it will become the Data Protection Act 2018.

[2] Information Commissioner's Office *Data sharing code of practice* (May 2011) at https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf

PART A: RECITALS

1. Scope of the Agreement

1.1 This Agreement sets out the top-level commitment by all Organisations and covers information sharing in any form and by any method, including paper, recorded and electronic formats. It applies to Personal Data, Sensitive Personal Data, Personal Confidential Data and non-personal information. It is based on their interpretation of the legal and ethical requirements for information sharing. It should not be construed as providing legal advice.

1.2 It supports section 251B of the Health and Social Care Act 2012 (which is inserted by s. 5 of the Health and Social Care (Safety and Quality Act 2015) which sets a duty for information to be shared where it facilitates care for an individual, and Article 26 of the EU General Data Protection Regulation (GDPR) by setting out the roles and responsibilities of Partner Organisations as Joint Controllers.

1.3 It applies to sharing among organisations and professionals. It does not cover communications between Health Professionals and individual patients, service users or carers.

1.4 This is the Overarching Information Sharing Agreement and as such provides the framework for Purpose Specific Information Sharing Agreement which enables the actual sharing of data. This agreement in and of itself does not facilitate sharing of data.

1.5 The Agreement encourages and promotes the sharing of information but does not alter the statutory duties of individual Organisations.

1.6 Adherence to this Agreement does not provide legal Exemption from data protection or any other legislation.

1.7 This Agreement will be underpinned by Purpose Specific Information Sharing Agreements between Organisations that are designed to meet the specific requirements for sharing specific information for specific purposes using specific systems.

1.8 This Agreement will be extended to other organisations working together to deliver services in South West London. Organisations entering an approved information sharing agreement will automatically become parties to this Agreement.

1.9 Where applicable, the terms used in this Agreement shall have the same meaning as in the GDPR.

1.10 References to guidance, standards and policy should be read as references to such guidance, standards and policy as updated from time to time.

2. Key legislation and best practice

2.1 The principles and procedures embodied in this Agreement are based on the rights of individuals under the following legislation and guidance.

2.2 The key legislation affecting the sharing and disclosure of personal information includes but is not limited to:

- Data Protection Act 1998 and 2018 (when it is enacted)
- (EU) 2016/679 General Data Protection Regulation (GDPR)
- Common law duty of confidentiality
- The Human Rights Act 1998
- Freedom of Information Act 2000
- National Health Service and Community Care Act 1990, now forming part of the NHS Act 2006
- Health and Social Care (Community Health and Standards) Act 2003, now forming part of the NHS Act 2006
- National Health Service Act 2006
- Local Government Act 1974
- Health and Social Care Act 2012
- Health and Social Care Safety and Quality Act 2015, now forming part of the NHS Act 2006
- Mental Health Act 1983
- Children Act 1989
- Children Act 2004
- Mental Capacity Act 2005
- Access to Health Records Act 1990
- Care Act 2014
- Crime and Disorder Act 1998
- Criminal Procedures and Investigations Act 1996
- Public Records Act 1950.

2.3 Guidance issued by the Information Commissioner and the following national health and care policy and guidance:

- NHS Constitution
- Confidentiality: NHS Code of Practice
- GMC "Confidentiality: good practice in handling patient information"
- NHS Care Record Guarantee for England
- Information Security. NHS Code of Practice
- HSCIC (now NHS Digital): "Code of practice on confidential information"
- National Data Guardian: "Information: To Share or Not to Share? The Information Governance Review" (2013) and "Review of Data Security, Consent and Opt-Outs" (2017)
- The Guide to Confidentiality in Health and Social Care.

3. The Agreement

This Agreement is endorsed by the signatories identified in Appendix A. This Agreement as between the parties is a non-legally binding memorandum of understanding.

3.1 The Organisations have agreed to lawfully share necessary information about their patients, service users and clients (who for convenience are all referred to in this agreement as "patients").

3.2 Processors processing data on behalf of the Controller must be held in contract by each party, either singularly or jointly.

3.3 By signing this Agreement each Organisation undertakes to implement and adhere to the principles, standards and governance set out in the Agreement, reassuring the other Organisations that Personal Data will be used and managed only in agreed and appropriate ways.

3.4 Each Organisation agrees that it is a Controller in respect of personal data that it discloses to other Organisations and is a Data Controller in Common when the information is shared.

3.5 Each Organisation is Controller for their organisation's information and solely responsible for obtaining its own legal assurance that it has a lawful basis for sharing the information it holds.

3.6 Each Organisation agrees that it is prepared to sign information sharing agreements for sharing specific information for specific purposes using specific systems.

3.7 The Organisations shall comply at all times with all Applicable Laws and regulations relating to processing of personal information and privacy in effect in England, and shall (where applicable) have regard to the guidance and codes of practice issued by the Information Commissioner (ICO), the Department of Health, General Medical Committee, the Health and Care Professions Council and other relevant regulators.

3.8 The Organisations confirm that they have:

3.8.1 Adequate information governance measures in place to ensure they can comply with this Agreement, and

3.8.2 Appropriate security measures to meet the requirements of GDPR Article 32

3.9 The Organisations shall not perform their obligations under this Agreement in such a way as to cause any other party to this Agreement to breach any of its obligations under Applicable Laws, regulations or guidance.

3.10 The Organisations agree to seek the permission of the originating Organisation if they wish to share Personal Data outside of the Partnership where possible.

3.11 Any Organisation may withdraw from this Agreement on giving written notice to Organisations under the provisions of section 18 below.

3.12 Regular reviews and audits of information will be undertaken to ensure that sharing meets the required objectives and obligations under this Agreement.

4. Principles

In all circumstances when sharing personal data, the following principles must be observed:

4.1 Personal Data will only be shared with organisations which are able to guarantee that they will meet the requirements of data protection and confidentiality privacy laws, observe professional ethics and protect the rights of individuals.

4.2 Personal Data will be shared lawfully, fairly and effectively for the Agreed Purposes to benefit individuals and services while protecting and respecting individuals' rights and freedoms.

4.3 Personal Data will be shared to the full extent permitted by law and in a manner compatible with the NHS Constitution and Caldicott Principles.

4.4 Confidentiality must be respected unless consent to disclose has been provided or there is a robust public interest or an alternative lawful basis for disclosure.

4.5 Decisions to share Personal Data will consider the impact this may have on the individual, their safety and well-being, and on others who may be affected by the decision to share.

4.6 Clear and accessible information will be provided explaining what Personal Data will be shared and how and why it will be used. **There should ordinarily be 'no surprises' to individuals about the use of their data.**

4.7 Personal Data shared will be adequate, relevant and necessary for the specific purpose for which it has been requested, and will only be shared with those people who need it for that purpose.

4.8 Every reasonable measure will be taken to ensure that Personal Data are accurate and, where necessary, kept up to date or corrected.

4.9 Only the minimum amount of Personal Data necessary for a specified purpose will be shared and will not be kept for longer than needed. If an objective can be achieved without fully identifiable Personal Data being shared, data will be de-identified or anonymised.

4.10 Personal Data will be protected against unauthorised or unlawful processing and against accidental loss, misuse, destruction or damage.

PART B: ARTICLES

5. Responsibilities of Partner Organisations (Recital 3.1)

5.1 Collectively Organisations are responsible for:

5.1.1 Reviewing and monitoring the effectiveness of the Agreement and amending when required;

5.1.2 Administering membership of, and compliance with, the Agreement;

5.1.3 Fostering a culture of information sharing among Organisations;

5.1.4 Supporting the development of purpose specific information sharing agreements;

5.1.5 Sharing and promoting best practice.

5.2 Individually each Organisation shall:

5.2.1 Ensure suitable representation and engagement through the Governing Group, collaborating with other Organisations as Joint Controllers to ensure that Personal Data will be shared lawfully, fairly and effectively to benefit individuals and services while protecting and respecting individuals' rights and freedoms;

5.2.2 Accept responsibility for independently or jointly auditing its own compliance with this Agreement and any Purpose Specific Information Sharing Agreements in which it is involved on a regular basis, at least twice yearly and provide assurance of compliance to the other Organisations;

5.2.3 Ensure that any purpose specific information sharing arrangement it is party to complies with legal and regulatory requirements and the provisions of this Agreement, including:

- ensuring all privacy and fair processing notices are up-to-date, available and accessible
- promptly notifying the Governing Group of any Security Incidents or Personal Data Breaches
- keeping and maintaining records of all requests for information sharing received and track the flow of Personal Confidential Data
- ensuring that Processors adhere to the principles, standards and governance set out in the Agreement, reassuring the other Organisations that Personal Data will be used and managed only in agreed and appropriate ways

5.2.4 Be responsible for reviewing their respective purpose specific information sharing agreements and providing assurance to the other Organisations that sharing information under this Agreement complies with the Agreement and meets the stated objectives.

5.3 Each Organisation will nominate a key contact to deal with queries and requests for information under this Agreement. This person shall also represent the Organisation in the Governing Group. The appointed contact shall usually be the Caldicott Guardian, Data Protection Officer, Information Governance Officer or equivalent.

5.4 The key contact for each Organisation will ensure dissemination of this Agreement in line with each Organisation's internal arrangements for the distribution of policies, procedures and guidelines and monitor the implementation and compliance of this Agreement within their own Organisation.

5.5 An Organisation may change its appointed contact at any time on written notice to the Governance Group.

5.6 It is the responsibility of each Organisation to ensure that details of its nominated contact are kept up-to-date on the central register of Data Protection Officers maintained by the Governing Group.

6. Information governance and assurance (Recital 3.1)

6.1 Organisations will determine their respective responsibilities for compliance with their obligations and apportion data protection compliance responsibilities in a transparent and accountable manner.

6.2 Any data stored in a shared environment or processed by Processors on behalf of the Controller will be managed under a written purpose specific information sharing agreement or contract.

6.3 Each Organisation shall have documented policies and procedures to ensure compliance with applicable requirements for data protection, information security and confidentiality and be committed to ensuring that any information is shared in accordance with its legal, statutory and common law duties, and, that it meets the requirements of any additional guidance.

6.4 All Organisations must adhere to robust information governance processes and data quality standards to protect patients and Organisations from exposure to risk. This should be supported by regular audits and an openness and accountability within the Governing Group of Organisations.

6.5 Each Organisation must ensure and maintain its registration with the Information Commissioner under regulations made further to the Digital Economy Act 2017and any registration requirements under subsequent legislation.

6.6 The Organisations will ensure that staff receive training and guidance, and abide by the rules and polices concerning the protection and use of any data covered by this Agreement.

7. Lawful basis (Recital 3.3)

7.1 When entering into purpose specific information sharing arrangements under this Agreement, the Organisations must identify the legal basis(s) for the proposed sharing and record this in the Information Sharing Agreement. The main sources of law governing the disclosure of personal and confidential data is:

- (EU) 2016/679 General Data Protection Regulation, Data Protection Act 2018
- Common law duty of confidentiality (and the Health and Social Care Act 2012)
- The Human Rights Act 1998.

The Organisations must also be mindful of any other legislation or legal principle relevant to them when sharing Personal Data including, but not limited to, legislation listed at section 2 above.

7.2 It is the responsibility of each Organisation to ensure that any information sharing arrangements it enters into has a lawful basis for processing, that all associated conditions and criteria are met, and that this is recorded as part of the information sharing agreement.

8. Individuals' privacy rights (Recital 3.5)

8.1 All sharing arrangements under this Agreement must be processed in way which respects and protects individual rights set out in Chapter III of the GDPR, the NHS Constitution and Caldicott Principles, including the rights to access, to have information about the nature of the processing and to opt-out.

8.2 A fair balance should be achieved between the public interest and the rights of the individuals.

8.3 The Organisations will ensure that principles of Privacy by Design are considered when planning new technologies, services or processes and, where applicable, Data Protection Impact Assessments are carried out.

8.4 It is the responsibility of the disclosing Organisation to ensure that information sharing agreements under this Agreement identify and set out applicable data subject rights and state how organisations will respect and allow individuals to exercise their rights.

8.5 If an Organisation receives a Subject Access Request under GDPR Article 15 (or any other attempt by a data subject to exercise their rights) and Personal Data is identified as belonging to another Organisation or third party, the receiving Organisation is responsible for contacting the original Controller promptly to invite their views on disclosure.

8.6 The response to Subject Access Requests relating to processing carried out under a purpose specific information sharing agreement will be the responsibility of the receiving party.

8.7 The Organisations will work together to investigate and remedy all complaints, and potential or actual data breaches or non-compliance with Data Protection Legislation.

8.8 Where processing is based on Consent under GDPR each Organisation must ensure that technical and organisational measures are in place to obtain and record Explicit Consent from patients and allow patients to select which elements of their information may not be shared. These measures must also allow for the patient to withdraw Consent and include a process for ceasing processing of such information immediately and give notice to affected Organisations. In cases where Consent has been obtained to provide a legal basis under GDPR there being no other applicable Article 6 or Article 9 conditions, this should be recorded.

8.9 Each Organisation must have a designated Data Protection Officer or Information Governance Manager who will be responsible for subject access requests.

9. Communication (Recital 3.6)

9.1 The Organisation**s shall ensure that fair processing and privacy notices are clear, consistent and accessible, and always available.**

9.2 Sufficient information will be provided for people to understand how their Personal Data is shared, with whom and why, and how to exercise any rights in respect of that data.

9.3 Each Organisation must effectively inform patients that they have the right to opt out of sharing their information or select or restrict which elements of their information may or may not be shared.

9.4 Each Organisation must effectively inform patients of the implications for the provision of care or treatment, such as the potential risks involved if their full record is not made available to Health Professionals involved in their care.

9.5 The Organisations will ensure that fair processing materials satisfy the recommendations of the Information Commissioner's Office guidance.

9.6 Each Organisation should employ a variety of channels to communicate with its patients regarding information sharing, such as information leaflets, posters, at the point of care, during the patient registration process or when referring into other services

10. Adequate and relevant (Recital 3.7)

10.1 Partner Organisations agree to process the minimum necessary data set to achieve the Agreed Purposes for Purpose Specific Information Sharing Agreement. Parties will consider the need for and benefits of more specific governance arrangements (i.e. a PSISA) for particular data sharing activities.

10.2 The nature and amount of data to be processed for the Agreed Purposes should be documented in Purpose Specific Information Sharing Agreements made under this Agreement.

11. Data quality (Recital 3.8)

11.1 Each Organisation is responsible for ensuring the accuracy of the data shared under the **Purpose Specific Information Sharing Agreement** for which it is the Controller.

11.2 Each Organisation must have in place documented systems to update any information if subsequently discovered to be inaccurate.

11.3 If an Organisation is aware of a material inaccuracy or omission in information that it shares under a **Purpose Specific Information Sharing Agreement**, that Organisation agrees to promptly alert sharing partners of that inaccuracy or omission.

11.4 The NHS number must be used as the unique patient identifier and systems used by the Organisations should connect to the Connecting for Health Personal Demographic Service to ensure the NHS numbers are accurate and demographic data synchronised.

12. Data minimisation (Recital 3.9)

12.1 Only the minimum information necessary for the purpose will be shared and, if sharing with providers, will only be shared when the **Purpose Specific Information Sharing Agreement** explicitly permits it.

12.2 Shared data may also be de-identified in accordance with all applicable law and guidance including, but not limited to, the BMA Confidentiality Toolkit and the Health and Social Care Information Centre Guide to Confidentiality. Wherever possible and practical anonymised or de-identified data will be used **to the extent that doing so would not compromise the objectives of the processing.**

12.3 The Organisations agree to maintain a written policy for the retention and disposal of information in accordance with the necessary legal framework and the "Records Management Code of Practice for Health and Social Care".[3]

13. Breach notification and security (Recital 3.10)

13.1 Each Organisation agrees to apply appropriate security measures to protect Personal Data in accordance with its obligations as a Controller and as required by GDPR Article 32 and in accordance with guidance produced by the ICO.

13.2 In the event of a Security Incident, Personal Data Breach or potential breach the responsible Organisation should immediately inform the Governing Group and all other affected Organisations with as many details as known at that time. Any affected Organisation (defined as the Controller of the Personal Data) shall investigate the Security Incident using that Provider's data loss or data breach procedures. Any affected Organisation shall update

[3] Information Governance Alliance: "Records Management Code of Practice for Health and Social Care" (2016) at https://digital.nhs.uk/article/1202/Records-Management-Code-of-Practice-for-Health-and-Social-Care-2016

the relevant Organisations and Governing Group, including the findings of any investigation report or remedial actions.

13.3 **The** Organisation**s agree to provide reasonable assistance and co-operation to facilitate the management of any incident in a prompt and compliant manner.**

13.4 All Organisations' systems under this Agreement must have processes in place to test, assess and evaluate the effectiveness of technical and organisational measures for ensuring the security of data processing activities.

13.5 If any Organisation cannot or may not be able to comply with the requirements in this clause, the partner should inform the Governing Group immediately. The Governing Group will undertake a review and may in its discretion authorise derogation from the above requirements subject to such conditions as it deems appropriate.

13.6 All Organisations' systems under this Agreement must have user authentication mechanisms to ensure that all instances of access are auditable against an individual, including where possible the following information:

- Job role and name of staff member accessing the system
- Organisation name
- What actions were performed and

The date and time the information was viewed.

13.7 The systems and technical measures used by each Partner Organisation for the sharing of Personal Data and Personal Confidential Data must be specified in any **Purpose Specific Information Sharing Agreement**.

14. Freedom of Information

14.1 The Organisations recognise that public bodies are subject to the requirements of the Freedom of Information Act 2000 ("FOIA") and the Environmental Information Regulations ("EIR"). Any such requests relating to this Agreement should be directed promptly to the Data Protection Officer or Information Governance Manager of the relevant Partner Organisation.

14.2 The receiving Organisations shall notify the Governing Group of any such request and assist and co-operate with the Governing Group to enable compliance with any obligations under the FOIA and the EIR.

14.3 A copy of this Agreement should be included in each Organisation's publication scheme.

15. South West London Information Governing Group

15.1 The South West London Information Governing Group comprising a representative of each Organisation or a representative of multiple organisations will oversee, support and maintain this Agreement.

15.2 Each Organisation will have a representative on the Governing Group which in accordance with clause 6.3 will be each Partner Organisation's key contact under this Agreement.

15.3 Individual members of the Governing Group shall act in accordance with their ethical and professional obligations.

15.4 The Governing Group will meet at least annually.

15.5 The Governing Group shall have the following powers and responsibilities:

15.5.1 To approve additional Organisations joining this agreement

15.5.2 To administer membership of this Agreement

15.5.3 To determine whether an Organisation should cease to be a party to this Agreement for a specific period or permanently for noncompliance

15.5.4 To determine whether an Organisation may derogate from or amend any requirement under this Agreement

15.5.5 To maintain an information conduit between the Organisations

15.5.6 To investigate breaches of the Agreement and require Organisations to take remedial actions

15.5.7 To monitor each Organisation's compliance with this Agreement. The Governing Group may request evidence of compliance with this Agreement on written request to any Organisation

15.5.8 To approve common patient and public communication materials and take a proactive role in ensuring effective communication about information sharing under this Agreement and

15.5.9 To develop, review and maintain this Agreement to ensure that it reflects any legal and statutory obligations and any other related best practice guidance in relation to information governance.

15.7 Governing Group decisions shall be taken by consensus. Before any Governing Group decision is taken, those taking the decision shall satisfy themselves that they are authorised to do so by those whom they represent.

15.8 If consensus on any decision cannot be reached, and unless the Governing Group decides otherwise, its decisions shall be taken by a simple majority. Where there is no majority the

Chair of the Group has a casting vote. If an individual represents more than one Organisation, that individual shall vote on the majority decision of those organisations they represent.

15.9 This Agreement will be reviewed every 2 years by the Governing Group, unless in the Governing Group's opinion new or revised legislation or national guidance necessitates an earlier review.

15.10 Following each review the Governing Group will confirm whether this Agreement remains fit for purpose, or whether to recommend amendments to the Partner Organisations.

16. Joining and withdrawing from the Agreement

16.1 Applications to become a signatory to this Agreement will be subject to the approval of the Organisations acting through the Governing Group.

16.2 Any Organisation may withdraw from this Agreement. The Organisation's signatory to this Agreement must notify the chair of the Governing Group in writing, stating the reason for withdrawal.

16.3 Where an Organisation wishes to withdraw due to concerns about the operation of this Agreement, the organisation should first raise its concerns with the chair of the Governing Group who will initiate an investigation. If the outcome of the investigation does not satisfy the Organisation, it may withdraw from the Agreement.

16.4 Applications from former Organisations to re-join the Agreement will be subject to clause 16.1.

17. Complaints and dispute resolution

17.1 The Organisations shall use all reasonable endeavours to work together to resolve any dispute or complaint arising under this Agreement or any data processing carried out further to it.

17.2 The Governing Group is responsible for investigating any concerns or complaints about the operation or content of this Agreement. Concerns should be raised in writing and evidence provided to the chairs of the Governing Group who will initiate an investigation.

17.3 Concerns or complaints about any **Purpose Specific Information Sharing Agreement** will be investigated and addressed through the Governing Group.

18. Sanctions

18.1 Any Organisation identified as breaching this Agreement may be removed from this Overarching Information Sharing Agreement pending investigation by the Governing Group.

18.2 Non-compliance with the terms of this Agreement by any Organisation may result in the Organisation or the Agreement being suspended or terminated by the Governing Group.

Appendix A - Signatories to this Agreement

SIGNATORY	DATE SIGNED
SWL GP Practices (Practices to be confirmed)	
Croydon Health Services NHS Trust	
St George's Healthcare NHS Trust	
Kingston Hospital NHS Foundation Trust	
Epsom and St. Helier's NHS Trust	
South West London and St George's Mental Health Trust	
Your Healthcare CIC	
London Borough of Sutton	
Royal Borough of Kingston upon Thames	
Sutton Health and Care Provider Alliance (from 1ST April 2019)	
Cerner Corporation	
EMIS Health	
In Practice (Vision)	

Appendix B – IG Working Group Membership as at 20-September-18

Name	Initials	Role and Organisation
Alan Ball	AB	Information Governance Manager, The Royal Marsden NHS Foundation Trust
Claire Clements	CC	IG SME, NELCSU
Dr Rod Ewen	RE	GP / Clinical IT Lead SWL Digital and Wandsworth CCG
Gillian Wood	GW	IG Expert, NELCSU
Janice Sorrell	JSo	Head of Information Governance, Kingston Hospital NHS Trust
Keith James	KJ	Head of Information Governance, St George's Hospital
Kevin Fitzgerald	KF	Chair and Director of IM&T, Kingston Hospital NHS Trust
Paul Kenny	PK	Information Governance Manager, Epsom and St Helier University Hospitals NHS Trust
Pera Svilar	PS	Deputy Information Governance Manager, Croydon University Hospital NHS Trust
Rachel Granger	RG	Digital Portfolio Manager, SWLHCP
Sally Fereday	SF	Interim Head of Corporate Services, SWL Alliance
Sally Wiltshire	SW	Interoperability Phase1 Project Manager, Nautilus/SWL Digital
Simon Evans	SE	Accounts Manager, Nautilus Consulting Ltd
Stephen Ifegwu	SI	Digital Programme Co-ordinator, SWL HCP
Tanya Campbell	TC	Information Governance Officer Adult Social care, London Borough of Sutton
Tanya Trimnell	TT	Health and Social Care Integration Project Manager, London Borough of Sutton
Thelma Sequeira	TS	Interim Digital Project Support Officer
Zoli Zambo	ZZ	Digital Project Manager, SWL HCP

Appendix C – SWL IG Working Group Terms of Reference

SWL%20IG%20Working%20Group%20Tol

Appendix D – SWL Interoperability Programme Phase 1 DPIA

DPIA Questionnaire V2_FINAL.docx

Appendix E - Glossary

Term	*Definition*
Applicable Law	Means any court order or any common law, statute, statutory instrument, order, regulation issued by a governmental body with authority over any relevant party, applicable to any relevant party from time to time in the context of its relevant rights and obligations under this Agreement and including the Data Protection Legislation.
Caldicott Principles	The principles set out in the 1997 and 2013 National Data Guardian reviews that health and social care organisations should use when reviewing their use of client information.
Consent	Means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.
Controller	Means a company, organisation or person who decides what data is collected, the purposes for which it is used and how that data is handled.
Data	Means the data including Personal Confidential Data to which a Provider Partner or a Provider Partner's contractor contributes and/or has access as a result of this Agreement.
Data Protection Impact Assessment (DPIA)	A systematic and comprehensive process for determining the privacy, confidentiality and security risks associated with the collection, use and disclosure for personal data prior to the introduction of or a change to a policy, process or procedure.
Data Protection Legislation	Means all Applicable Laws and regulations relating to processing of personal data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner or any NHS regulatory or advisory body, including but not limited to the Caldicott Reports relating to the sharing and processing of patient data.
Data Subject	Means the person who is the subject of the Personal Data.
De-identified Data	Has the same meaning as pseudonymised data under the GDPR, namely, the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Term	*Definition*
Explicit Consent	Means articulated patient agreement which gives a clear and voluntary indication of preference or choice, usually given orally or in writing and freely given in circumstances where the available options and the consequences have been made clear for the specific details of processing; the data to be processed; and the purpose for processing.
Governing Group	Means the group defined in clause 17 of Part B of this Agreement (South West London Digital Information Governing Group.
Health Professional	Means an individual who is employed or engaged by a Provider Partner and is either: (a) a regulated or registered health or social care professional involved in the direct care of, or (b) an individual co-ordinating or facilitating direct care for a person receiving services in North West London
Information Sharing	Information sharing, in the context of this policy, means the disclosure of personal information from one or more organisations to a third party organisation or organisations, or information shared internally within an organisation. Information sharing can take the form of: • a reciprocal exchange of data • one or more organisations providing data to a third party or parties • several organisations pooling information and making it available to each other • several organisations pooling information and making it available to a third party or parties • exceptional, one-off disclosures of data in unexpected or emergency situations.
Information sharing agreements	Sets out a common set of rules to be adopted by the various organisations involved in a data sharing operation. For the purposes of this document, the term includes data protection clauses in contracts. [ICO *Data Sharing Code of Practice*]
Integrated Care Records	Means the Whole Systems Integrated Care Record and the CIE Care Record. An Individual Integrated Care Record is the integrated care record for each individual patient, amalgamated from Data derived from each Provider Partner's source systems which may be accessed by Provider Partners for Direct Care.
NHS Information Governance Toolkit (IGT)	Means the set of information governance requirements produced by the Department of Health and now hosted by the Health and Social Care Information Centre. It is a tool with which health and social care organisations can assess their compliance with current legislation and national guidance.
Partner Organisations	Means the organisations party to this Agreement.

Term	*Definition*
Personal Confidential Data	Means personal information about identified or identifiable individuals, which should be kept private or secret. For the purposes of this Agreement 'personal' includes the definition of 'Personal Data', but it is adapted to include dead as well as living people. 'Confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'Sensitive Personal Data' as defined in this Agreement.
Personal Data	Means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Personal Data Breach	Has the same meaning as in the GDPR Article 4(12) that is, a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.
Processor	Means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.
Provider Partners	All the Partner Organisations who provide health or social care; for the avoidance of doubt this does not include PKB or Brent CCG
Security Incident	Means any incident which results or could potentially result in: • unauthorised or unlawful processing of Personal Data • accidental loss, destruction, corruption or damage to Personal Data • the confidentiality, integrity or availability of Personal Data being compromised • network or information systems becoming unavailable or compromised as the result of a data security or cyber security event • breach of any privacy or data protection requirements.
Sensitive Personal Data	Has the same meaning as 'special category' in the GDPR Article 9(1), that is, personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Term	*Definition*
Whole Systems Integrated Care Record or WSIC Record	Means the shared electronic integrated care record collating coded patient information stored in a centralised data warehouse maintained by the Host related to the delivery of health or social care of patients of Provider Partners and to which Provider Partners will have access in accordance with the provisions of Part A of this Agreement.

References

Legislation

Civil Contingencies Act 2004

Data Protection Bill

Environmental Information Regulations 2004

Freedom of Information Act 2000

Health and Social Care Act 2012

Health and Social Care (Safety and Quality) Act 2015

Human Rights Act 1998

Regulation (EU) 2016/679 (General Data Protection Regulation)

Guidance and Codes of Practice

British Medical Association (BMA) Confidentiality Toolkit
https://www.bma.org.uk/advice/employment/ethics/confidentiality-and-health-records/confidentiality-and-health-records-tool-kit

Department of Health
NHS constitution for England (27 July 2015)

General Medical Council (GMC):
Confidentiality: good practice in handling patient information (2017)

Information Commissioner's Office:
Data sharing code of practice (2011)

Information Governance Alliance
Records Management Code of Practice for Health and Social Care (2016)

National Data Guardian
Information: To share or not to share? The Information Governance Review (March 2013)
Review of data security, consent and opt-outs (July 2016)

NHS Interoperability Toolkit (version 2) at https://digital.nhs.uk/interoperability-toolkit

NHS Digital Information Governance Toolkit at https://www.igt.hscic.gov.uk/

North West London Care Partnership website at
https://www.healthiernorthwestlondon.nhs.uk/bettercare/thevision/partnership