North West London
Whole Systems Integrated Care

Whole Systems Integrated Care

Privacy Impact Assessment Report

Please note this is a living document and will be reviewed regularly by the WSIC ISA Governance Group

Document Information

Title:	NWL Whole Systems Integrated Care PIA Report
Project:	WSIC
Document owner(PM):	WSIC ISA Governance Group
Document author:	Debbie Terry
Date created:	19th March 2015
Current status:	Version 1 of a living document
File name:	WSIC PIA v1.0 FINAL 190315

Version History

Version	Date issued	Updated by	Reason
0.1	03/03/15	Debbie Terry	Issued for comment
0.2	18/03/15	Debbie Terry	Issued final draft for comment
1.0	19/03/15	Debbie Terry	Final version issued
1.1	14/04/2015	Selin Barnett	WSIC ISA Governance Group Feedback

Client Contacts

Distributed to	Commented (version and date)
Selin Barnett	0.1 – 09.03.15
David Stone	0.1 – 09.03.15
Selin Barnett	0.2 – 19.03.15

North West London
Whole Systems Integrated Care

1 Contents

1 Introduction

1.1 Background Information.

This Privacy Impact Assessment (PIA) applies to the North West London Whole Systems Integrated Care (WSIC) programme. North West London is one of fourteen national Integrated Care Pioneers leading the way forward to drive change within health and social care services, acting as exemplars to others in their use of ambitious and innovative approaches. The overall ambition of the NWL programme is to achieve better outcomes for patients/service users and their carers through the development and delivery of more integrated care by working together, pooling budgets and agreeing new ways of organising health and social care service provision.

Integrated care is dependent of the availability of quality information to support:

a) The linkage and sharing of service user information between the various direct care settings and making it available to front-line professional staff at the point of need in order to inform decisions and support better care delivery (direct care);
b) Expert analysis of information derived from service user activity to provide quality data for commissioners and providers and used to plan, implement and manage integrated health and social care services (indirect care).

The use of personal information is subject to the principles of the Data Protection Act 1998 and common law duty of confidence. Public bodies also need to be aware of their responsibilities under the Human Rights Act 1998, in particular Article 8 of the European Convention of Human Rights which guarantees a right to respect for a private life.

In summary:

- Patients/service users have the right to privacy and confidentiality and to expect the NHS to keep their confidential information safe and secure;
- Staff have both a professional and legal duty to keep information provided to them in the course of care delivery confidential and to respect privacy[1]
- Commissioners need information derived from service user activity to (amongst other things) pay services, measure and evaluate the quality and effectiveness of care, identify service requirements and assess the impact of their decisions.
- Organisations have corporate responsibility and a legal duty to ensure their activities, and the activities of their staff in the in the use of personal data comply with national law, policy and guidance.

1.2 Why do we need to do a Privacy Impact Assessment?

[1] Section 3a of the NHS Constitution – See the NHS Constitution Handbook for detailed explanation https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/170649/Handbook_to_the_NHS_Constitution.pdf

A PIA is a systematic process that is used to analyse privacy law compliance within a system, which helps to identify, understand and manage or reduce the privacy risks whilst allowing the aims of the project to be met.

Privacy risk is the risk of harm arising through an intrusion into privacy e.g. via a breach of confidentiality, and includes both risks to the individual and corporate risk arising from non-compliance with legal obligations and reputational harm.

This PIA follows the Information Commissioner's Conducting Privacy Impact Assessment Code of practice
https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf

1.3 Assumptions.

The WSIC programme started in 2013 when NWL succeeded in their application to become an Integrated Care Pioneer. The first two years have been spent designing the system and preparations are being made to start implementing local plans from April 2015[2].

This PIA is being conducted in preparation is for the next stage of the WSIC programme, with a particular focus on looking towards a future state when all information requirements are supported by a digital integrated care system.

The future state WSIC IT system to support health and care professionals in the delivery of direct care has yet to be specified and developed. This PIA has been completed using various information available at the time i.e. Information Sharing Agreement and supporting documents[3] as well as information provided by members of the Governance Group, however there are some unknowns at this stage.

Certain assumptions have therefore been made about the way in which the system will work, for example, it will have the technical ability to record patient consent decisions to control the use of their confidential information; control individual access levels down to a specific role restricted to justifiable "need to know" levels of data; and include robust audit trails to enable the prevention and detection of unauthorised access etc. It is made clear throughout this document where such assumptions have been made.

Personal data downloaded from various Provider Partner systems into the WSIC system for ***direct care*** purposes flows on a basis of ***implied*** patient consent. The patient's GP is responsible for organising and coordinating the care package and is therefore also responsible for obtaining their patient's ***explicit*** consent to activate the record and share information between the ***direct care team***.

For the purposes of understanding this PIA:

[2] See the NWL WSIC "Our Journey" for further information about the project http://integration.healthiernorthwestlondon.nhs.uk/
[3] See 2 - Resources

The term "patient" is used throughout this document but is interchangeable with "individual," "client", "service user" or "customer" i.e. an individual who is receiving integrated health and/or social care. There is no agreed generic term for an individual being cared for in an integrated care system.

Implied consent means:	Having been provided with information to explain to patients' how their personal confidential data will be uploaded into the WSIC system and used to support their direct care, the patient's agreement will be assumed unless they take action to inform their GP they do not agree and register their objection i.e. they opt-out.
Explicit consent means:	A positive response to a specific request for permission expressed verbally, in writing or other means of communication.

It is NHS policy that implied consent can only apply to sharing information for a direct care purpose, because that usage is within the scope of a patient's understanding and expectation. [4]

Direct Care means:	A clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals. It includes supporting individuals' ability to function and improve their participation in life and society. It includes the assurance of safe and high quality care and treatment through local audit, the management of untoward or adverse incidents, person satisfaction including measurement of outcomes undertaken by one or more registered and regulated health or social care professionals and their team with whom the individual has a legitimate relationship for their care (*the "direct care team"*).
Indirect care means:	Activities that contribute to the overall provision of services to a population as a whole or a group of patients with a particular condition, but which fall outside the scope of direct care. It covers health services management, preventative medicine, and medical research. Examples of activities would be risk prediction and stratification, service evaluation, needs assessment, financial audit.[5]

It is assumed that the reader will be familiar with the Data Protection Act 1998 terminology used throughout this document. A Glossary is provided for reference at the end of this document.

[4] Independent Information Governance Review (Caldicott 2) Report Section 3.2 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf

[5] Independent Information Governance Review Report 2013 (Glossary Page 129)

1.4 Abbreviations

Acronym	Description
CAG	Confidentiality Advisory Group
CCG	Clinical Commissioning Group
CSU	Commissioning Support Unit
DH	Department of Health
DPA	Data Protection Act 1998
DSCRO	Data Services for Commissioner's Regional Office (part of HSCIC)
GP	General Practitioner
HRA	Human Rights Act 1998
HSCIC	Health and Social Care Information Centre
LA	Local Authority
NHSE	National Health Service England (The Commissioning Board)
NWL	North West London
WSIC	Whole Systems Integrated Care

1.5 Partners

The North West London Whole Systems Integrated Care (WSIC) programme is a partnership between the organisations listed below:

- Lay Partners Advisory Group;
- Brent Clinical Commissioning Group (CCG);
- Central London CCG;
- Ealing CCG;
- Hammersmith and Fulham CCG;
- Harrow CCG;
- Hillingdon CCG;
- Hounslow CCG;
- West London CCG;
- GP Practice members of those CCGs listed above;
- Central London Community Healthcare NHS Trust;
- Central and North West London NHS Foundation Trust;
- Chelsea and Westminster Hospital NHS Foundation Trust;
- Hounslow & Richmond Community Healthcare NHS Trust;
- Imperial College Healthcare NHS Trust;
- The Hillingdon Hospitals NHS Foundation Trust;
- West London Mental Health NHS Trust;
- West Middlesex University Hospital NHS Trust;
- NHS England;
- Brent Council;
- City of Westminster;
- Ealing London Borough Council;
- London Borough of Hammersmith & Fulham;
- Harrow Council;
- London Borough of Hounslow;
- The Royal Borough of Kensington & Chelsea;

1.6 Status of this document and review

A PIA completed in the early stages of a project enables privacy to be designed into the system, however, this should be a reiterative process to compensate for what is unknown at the point of the first assessment and the inevitable changes that occur during a program's lifecycle.

This document therefore is a progressive living document that needs to be regularly refreshed and reviewed during the lifecycle of the programme. Initially (and especially in view of the current pace of change) review is recommended on a regular basis e.g. quarterly moving progressively to an eventual annual basis.

The Governing Group are the appropriate body to decide whether or not to accept the recommendations and initiate action as appropriate.

The Governing Group is also the appropriate body to ensure the review of this PIA as advised.

2 Privacy Impact Assessment

2.1 Project General Details

Name:	North West London Whole Systems Integrated Care programme
Objective:	The overall aim of the WSIC Programme is to improve the quality and effectiveness of care for individuals, carers and families across North West London by integrating health and social care services and resources.
Background: Why is the new system / change in system required?	The current system is fragmented, ineffective and does not make the best use of limited resources. Key information about individual service users is not shared between health and social care organisations appropriately to support direct care purposes; or not available for analysis and effective management of public services and limited resources.
Benefits:	The creation of an 'Integrated Care Record' will support multidisciplinary health and social care working by ensuring information is available to inform decisions about an individual's care and treatment at the point of need. This will also enable patients to be better engaged as partners in their care by being informed, improving their participation in decisions made about them, and give them more autonomy. Health and social care professionals will be able to keep the wider care team updated via the integrated care record. The quality and effectiveness of care will be improved. "The wider direct care team" - will benefit from receiving timely information about their patients from other care providers and settings. Information to support better care planning will reduce the number of unplanned admissions and emergency care. Data is provided to: • Inform the planning, development and improvement of care; • Manage the system more effectively i.e. activity, cost, operational performance and quality of service • Allow commissioners to set integrated capitated budgets, enabling the movement of resources across the system, reduction of waste and provide an incentive to take collective accountability for resources and outcomes
Constraints	Political expectations of innovative and ambitious Pioneers Lack of reliable central IG guidance and support May General Election (more change ahead?) Public anxiety (various issues) Multiple stakeholders moving at different paces
Relationships:	A list of partners is provided at section 1.4

Quality Expectations	Information will be of a quality to accurately support the business objectives	
Cross reference to other projects:	Shaping a Healthier Future (SHaFT)	
Programme Manager:	Name:	Sonia Patel
	Title:	Strategy & Transformation Informatics Lead
	Department:	Strategy & Transformation
	Telephone:	07977078237
	Email:	sonia.patel@nw.london.nhs.uk
Information Asset Owner:	Name:	Bernard Quinn
	Title:	Director of Performance and Delivery
	Department:	Performance and Delivery
	Telephone:	020 8966 1029
	Email:	Bernard.Quinn@nhs.net
Information Asset Administrator:	Name:	Jason Clarke
	Title:	Risk and IG Manager
	Department:	Governance
	Telephone:	0208 966 1093
	Email:	jasonclarke@nhs.net
Deputy Information Asset Administrator:	Name:	Keith Dickinson
	Title:	Head of Governance
	Department:	Governance
	Telephone:	0208 966 1141
	Email:	Keith.dickinson1@nhs.net
Customers and Stakeholders:	All organisations and individuals involved in the delivery of health and social care services. The population of NWL.	

2.2 Privacy Impact Assessment Key Questions

The first stage of a PIA is to complete a series of screening questions which are designed to:

a) Identify whether or not a PIA is necessary (it will always be necessary where personal data is being processed): and
b) Focus on the key areas for assessment.

The screening questions are provided in Appendix 2.

2.3 Key areas for assessment:

Patient information is extracted from GPs and service provider systems e.g. community, acute hospital, mental health and social care (collectively termed the “Provider Partners”), which is linked to form the Integrated Care Record held in the WSIC system and used for the purpose of direct care provision.

Service user activity data is de-identified to populate the Integrated Care Commissioning dataset and used for indirect care (commissioning) purposes.

A legally binding WSIC Information Sharing Agreement signed by all Provider Partner establishes the statutory, mandatory and best practice terms and conditions that underpin and control access and use of the system.

All Provider Partners are data controllers who act either alone or in common with other data controllers.

Data Processors have been engaged to operate the technical systems and process personal data on behalf of the data controllers.

A Governing Group has been established to oversee the management of the ISA and its subsequent application and development, ensuring all data controllers are engaged and decisions that impact the whole system are made in consultation and with their agreement.

2.4 Legal compliance assessment

Any use (processing) of personal data has to have a lawful basis covering the common law duty of confidentiality, the Data Protection Act 1998 (DPA) and Human Rights Act 1998 (Article 8) (HRA).

The approach is to firstly ensure there is a common law basis under which to operate and secondly assess compliance with the data protection principles. If both are satisfied then the HRA requirements will also be met.

The full details of the legal compliance analysis and conclusions can be found in Appendix 3**.**

2.5 Key risk areas identified by the PIA are:

- Compliance with the common law duty of confidence;
- Compliance with the DPA fair processing and lawfulness conditions;
- Unable to accurately assess compliance with the third data protection principle;
- Non-compliance with the sixth principle identified
- Assurance/transparency in data controller/data processor arrangements required
- Dependency on mitigation of risks (as above) to secure compliance with the HRA

3 Conclusions – Executive summary

The Recommendations set out in section 4 indicate where improvements can be made to strengthen existing information governance measures and ensure more robust compliance with the privacy laws and standards of practice.

3.1 The PIA identified one non-compliance risk concerning the sixth data protection principle – processing personal data in accordance with the rights of the data subject. This concerns the right of access to personal data (known as Subject Access Requests or SARs). Current arrangements are to refer an individual requesting access to their records back to the source provider of their personal data. The combination of data pooled for view in the

Integrated Care Record is a sub-set of the Provider Partner data-set and an "accessible" record by PA definition. It would be unlawful to refuse to provide an individual patient with a copy of their WS Integrated care record and the Information Sharing Agreement needs to be updated to include a central point for dealing with SARs. Direct patient access in the future will probably eliminate the formal system of requesting access to records.

3.2 There were concerns about the lawful basis for some of the data flows that questioned the reliance on implied patient consent, however this may be due to the absence of more detailed information and assumptions made on how the system will work. It is probable that these will be resolved when the existing reliance on various Secretary of State approvals to process patient data will change under new incoming Regulations. However, these are highlighted in order for the Governing Group to focus their attention to ensure future-state operates lawfully when the details of these changes are known.

3.3 It is, however, necessary to review the information provided to patients to secure informed consent. The patient right to object to their personal data being processed for in-direct care purposes is not currently transparent and there is an increasing need to address this. It should already be in place as a condition of the s251 approvals that have supported data flows since 2013; a condition of the recent s251 approval to cleanse and link GP data to commissioning data if that option is taken; and most likely to be a condition for processing set out in the new Regulations.

3.4 Finally, it is recommended that this PIA should be considered to be a progressive living document that undergoes regular review by the Governing Group to ensure privacy by design is built into the future state WSIC system.

4 Recommendations

No	Appendix 3 Section	Page	Recommendation
1	Common law duty of confidence	20	Improve transparency and openness by reviewing the "Resources" information on the WSIC website designed to inform patients about the uses of their personal data, to ensure it is free from codes and acronyms that an ordinary person would not reasonable be expected to understand. Seek advice from the Lay Partners Forum to test all publications are clear, relevant and understandable.
2	Common law duty of confidence	21	A documented procedure and script should be developed to guide front-line staff in how to obtain explicit patient consent and record opt-out codes into the GP system to ensure individual patient choice is upheld. The script should include appropriate wording to (a) explain choices available to them and what questions to ask to obtain explicit consent; and (b) explain the impact to their direct care if a patient dissents, including appropriate action to be taken when an opt-out

			decision has to be overridden.
3	Common law duty of confidence	22	Develop a WSIC Patient Consent Management Strategy and provide practical guidance for GPs in how to approach patients and manage their respective choices. Supporting communication materials for patients must clearly explain their NHS Constitution rights to object to their personal data being used for in-direct care purposes
4	Common law duty of confidence	22	The WSIC Patient Consent Strategy should identify all consent and opt-out requirements and ensure future-state systems can support various levels of patient choice.
5	Common law duty of confidence	22	The Governance Group should reconsider the lawful basis for processing patient confidential data for a "case finding purpose" as the reliance on implied consent does not appear to meet national or professional guidance. The outcome should inform the WSIC Patient Consent Strategy.
6	Data Protection Act	26	Develop a communications plan to support the GP Practice Data Controllers in their duties to ensure their registered patient population are adequately informed and have a reasonable period of time in which to register any objections before data is extracted for the WSIC system.
7	Data Protection Act	26	The Governing Group should review the Information Sharing Agreement section 8 to either (a) permanently delete data held in the WSIC when a patient registers an objection, or (b) inform the patient of the intention to hold hidden data for a period of six months and allow them to raise a further objection if they do not they agree to that.
8	Data Protection Act	28	The Governing Group are advised to be aware of the conditions for processing personal data and regularly review the WSIC data flows against changing circumstances to ensure there is a current and future legal basis to support the usage and proposed usage of data. It is also important to be aware of the requirement to inform patients about their right to object to secure any legal basis relied upon.
9	Data Protection Act	31	The clear purpose for the WSIC system should be determined, following which the data items in the Data Schedules should be reviewed to ensure they are relevant, proportional and necessary to meet that purpose. The RCP Guidance should be followed to determine the content of the Integrated Care Record.
10	Data Protection Act	32	A whole systems procedure for managing inaccuracies in the Integrated Care Record focussed around a central point of contact to support front line staff in the reporting and correction of data should be established. The procedure should be documented to identify responsibilities and provide clear instruction to staff to ensure a consistent approach.
11	Data Protection Act	33	The system specification should include future-state capability to ensure a full digital integrated care record that supports real time entry of clinical information**.**
12	Data Protection Act	34	Data should be retained in accordance with the NHS Records Management Code of Practice in a format that enables it to be reproduced in accordance with recognised medico-legal standards for the lifetime of that record. Assurances that this requirement will be included in future state systems is essential and therefore must be included in system specifications.
13	Data Protection	35	The Governing Group are advised to review the Information Sharing Agreement section 6.5 decision on arrangements for dealing with

	Act		subject access requests. The Integrated Care Record held in the WSIC system is an accessible record and patients have a legal right to be provided with a copy upon request.
14	Data Protection Act	37	The Governing Group should review the existing data controller/data processor contracts to ensure they (a) clearly identify those data controllers the contract applies to and (b) clearly include the DPA seventh principle conditions for information security. The contracts should be subsequently reviewed on an annual basis (or earlier if circumstances dictate)
15	Human Rights Act	38	This PIA is a progressive living document and should be reviewed on a regular basis by the Governing Group on a regular basis (every 3 months initially moving towards an annual review when stable) to ensure remedial actions are taken as recommended and the outcomes and risks are considered in line with legal changes and developing guidance.

Appendix 1 – Privacy Impact Assessment Key Questions

Question	Response
Will the system ('asset') contain personal identifiable data and/or sensitive personal data?	[ ] No [X] Patient [X] Staff [ ] Other (specify) Includes both personal data and sensitive personal data about patients/service users, and personal data about staff within the direct care team.
Please state purpose for the collection of the data. **for example, patient treatment, health administration, research, audit, staff administration**	Information collected from GPs and service providers e.g. community, acute hospital, mental health and social care will form the integrated health and social care record held in the WSIC system and will be used for the purpose of direct care provision. De-identified data derived from service user activity data will populate the Integrated Commissioning dataset and used for indirect care (secondary use) purposes. to support the establishment of Accountable Care Partnerships (ACP's)
Does the asset involve new privacy-invasive technologies. **e.g. visual surveillance, digital image and video**	[ ] Yes [X] No

recording, profiling, data mining, and logging of electronic traffic	
Identify the data items that are held in the system	Personal data and sensitive personal data will be held in the system. See the WSIC Data sets + exclusion codes http://integration.healthiernorthwestlondon.nhs.uk/resources
What checks have been made regarding the adequacy, relevance and necessity for the collection of personal and / or sensitive data for this asset?	• Data templates produced by all data controllers • Governance Group oversee the changes to the agreed data templates and Information Sharing Agreement. • No changes are made without agreement from the data controllers • View is determine by clinical need The plan is to extract codified data from care systems i.e. there will be no data extracted from free text fields. Future state - The assumption is that the full MDS identified by the data flow mapping exercise to inform the system specification, will be reviewed by the data controller members of the governance group to justify adequacy, relevance, necessity etc. for the purpose of and agreed with all stakeholders prior to its collection and use in the WSIC system.
Is the third party contract/supplier of the system registered with the Information Commissioner? What is their notification number?	[X] Yes [ ] No Data Protection Act (DPA) Notification Number: **Brent CCG ZA008025** **Concentra Z1711430** **South East CSU (hosted by NHS England) Z2950066** **Egton Medical Information Systems Z5514037** **Pheonix Partnership Z1927388**

	NB. These are data processors, processing personal data on behalf of the data controllers under contract. The data controllers remain responsible for compliance with the DPA and also need to be appropriately registered with the ICO.
Do the third party contract / supplier contracts contain all the necessary Information Governance clauses including information about Data Protection and Freedom of Information?	☐ Yes ☐ No Contract arrangements need to be more visible – couldn't complete this section in absence of relevant information. ISA established between Data Controllers and Brent CCG which includes sub-contractor instructions.
Are you relying on individuals (patients/staff) to provide consent for the processing of personal identifiable or sensitive data?	☒ Yes ☒ No Intention is to operate on a consent to view system for direct care when the system is operational.
If yes, how will that consent be obtained? Please state:	The system has to be designed, but the plan is to flow data from the GP system/Provider system relying on informed implied consent which includes an option for those who do not want an integrated care record created to opt-out. Stage 1 Informed implied consent for upload Consent is not necessary where there is a direct care purpose, but this assumes everything has been done to ensure the patients are adequately informed and have had an opportunity to register any objection. Stage 2Front line staff who have a legitimate relationship with the individual will ask for explicit consent from the patient to allow access to their ICR by them or the MDG team treating them. Initially consent is registered in the GP system, A NWL system of recording consent is being developed The procedure for access to records for patients who lack the capacity to consent is in line with national guideline.

How will the information be kept up to date and checked for accuracy and completeness?	Each individual data controller will be responsible for their own data quality and required to ensure data is of a quality fit for purpose. GP and social care data in the WSIC system will only be as accurate or complete as that extracted from the source systems. Feeds taken from national data sets i.e. SUS, SLAM, MHMDS ensures data quality of secondary care data. Future state- refresh every 24 hours expected. The theory is that health care professionals, or patients who identify an inaccuracy within a record should inform the original data controller who is responsible for ensuring it is updated/corrected. It is not clear how this will work in practice and supporting policy/procedure to support local governance of the system should be developed.
Who will have access to the personal data?	Access to personal confidential data will be restricted through role based access controls to health and care professionals and support workers who are members of the direct care team and have a legitimate relationship with the individual being cared for.
Do you intend to send direct marketing messages by electronic means? This includes both live and pre-recorded telephone calls, fax, email, text message and picture (including video)?	[ ] Yes [X] No This activity is regulated by the Privacy and Electronic Communication Regulations 2003 which are generally based on the requirement to obtain consent.
Is automated decision making used? If yes, how do you notify the individual?	[ ] Yes [X] No
Is there a useable audit trail in place for the asset. For example, to identify who has accessed a record?	[X] Yes [ ] No The asset has yet to be developed – future state will link in Patient Knows Best.
Have you assessed that the processing of personal/sensitive data will not cause unwarranted damage or distress to the individuals concerned? What assessments has	[X] Yes [ ] No Stakeholder engagement indicates patients expect/require health and care professionals to have access to relevant information to support direct care. Opt-out is available and explained in all communication materials.

been carried out?	Each data controller will be responsible for managing patient opt-out requests. A central, project record of the number of patients choosing to opt-out will enable the Governance board to monitor public confidence in the system e.g. by benchmarking with other comparable projects.
What procedures are in place for the rectifying/blocking of data by individual request or court order?	Contractual condition in ISA is that each data controller is responsible for complying with requests under the DPA 1998 – Clauses 3.7 & 8.1 Coded opt-out process blocks data flowing from data controller systems into WSIC system. Subsequent rectification blocking etc. of data already extracted would be updated at the next data extraction.
What procedures are in place to support subject access requests?	Each data controller is responsible for responding to SARs (ISA section 6.5). Future state patients will have direct access to their own records held on the system (PKB). An interim solution to deal with access requests to the integrated care record held centally on the WSIC nees to be established.
Does the asset involve changing the medium for disclosure for publicly available information in such a way that data becomes more readily accessible than before? (for example, from paper to electronic via the web?)	☐ Yes ☒ No Data will not be made publicly available.
What are the retention periods (what is the minimum timescale) for this data? (please refer to the Records Management: NHS Codes of Practice)	Retention periods are governed by Department of Health Policy and it is assumed these will be adhered to by all data controller parties.
Will the information be shared with any other commercial businesses?	☐ Yes ☒ No

	There is no intention to share the information with any business other than those included in the WSIC programme and signed up to the NWL Information Sharing Protocol.
Does the asset involve new linkage of personal data with data in other collections, or is there significant changes in data linkages?	[X] Yes [ ] No Data extracted from the various different provide systems will be linked to create the integrated care record.
Where will the information be kept/stored/accessed?	In the interim the data will be stored in the CSU Data Warehouse moving onto the long term Hitachi solution in July 2015
Please state by which method the information will be transported/ secure	SFTP or encrypted email
Are you transferring any personal or sensitive data to a country outside the England? **If yes, where?**	[ ] Yes [X] No
Is there a system level security policy in place for the asset?	[X] Yes [ ] No CSU security policy - infrastructure hosted Brent CCG

Is there a contingency plan/backup policy in place to manage the effect of an unforeseen event? **Please provide a copy.**	[ ] Yes [X] No DR & BCP fall over – CSU infrastructure CCG's Business Continuity plans and risk register.

Are there procedures in place to recover data (both electronic/paper) which may be damaged through: **Human Error** **Computer virus** **Network failure** **Theft** **Fire** **Flood** **Other disaster** **Please provide policy titles**	[X] Yes [ ] No All data held in the system is a duplicate – in the event of a failure recovery procedure will revert back and extract a copy of the source data.
Form Completed by:	**Debbie Terry** **Principal Consultant** **Kaleidoscope Consultants**
Signature: **Date:**	

Appendix 3 Legal Compliance Assessment

Any use of patient data needs to have a lawful basis covering the Data Protection Act 1998, the Common Law Duty of Confidentiality and take account of the Human Rights Act 1998 (Article 8).

Part 1 Common Law duty of Confidence.

Any use of confidential personal data must be lawful. There are four legal bases for processing personal confidential data which meet the common law duty of confidentiality. These are:

- *with the consent of the individual concerned;*
- *where another law provides a power to collect confidential data without consent e.g. section 251 of the NHS Act 2006 and the powers given to the Information Centre in the Health and Social Care Act 2012;*
- *through a court order where a judge orders that information should be disclosed; and*
- *when the processing can be shown to meet the 'public interest test', meaning the benefit to the public of processing the information outweighs the public good of maintaining trust in the confidentiality of services and the rights to privacy for the individual concerned.*

For consent (both implied and explicit) to be both legal and ethical it must be given by a person who has:

- *the capacity to make a decision;*
- *been provided with enough information to be adequately informed;*
- *voluntarily agreed i.e. not been coerced or unduly influenced; and*
- *has been given a fair choice.*

In addition to having one of these legal bases the processing must also meet the requirements of the DPA and pass the additional tests in the Human Rights Act 1998 (HRA).

Any processing of personal confidential data that is not compliant with these laws, even if otherwise compliant with the DPA, is a data breach. An organisations' failure to comply with the law when dealing with people's personal confidential data erodes the public's trust, damages reputation and risks enforcement action being taken by the Regulator(s) and legal action being taken by the individual whose privacy has been compromised.

The NHS operates mainly on a basis of implied consent to support the common law requirements when sharing personal confidential data between care professionals providing direct healthcare and treatment.

For implied consent to be legally valid, the patient must be informed and have an opportunity to express their dissent. If a patient does not raise an objection then their agreement to the sharing of their information may be implied. Most patients will understand and accept that information is shared within a healthcare team looking after them, but steps must be taken to explain disclosures that they would not reasonably expect

to happen. Implied consent can only apply to direct care[6]. Explicit consent is required for any use of personal confidential data beyond a direct care purpose.

A patients' right to object to their personal data being used for indirect care purposes is derived from common law and the Human Rights Act 1998 and confirmed in the NHS Constitution 2013.[7] Patients can object to:

- information about them leaving a general practice in identifiable form for purposes other than direct care; and
- information about them leaving the HSCIC in identifiable form, (confidential information about them will not be sent to anyone by the HSCIC).[8]

Public engagement has indicated positive support for the WSIC programme[9]. Information has been actively communicated to the local population to inform them about the intention to share their personal confidential information between organisations providing care and treatment. (Also see "Fair Processing" in the DPA section).

The communications materials are designed to inform the local public about the intended use of their information for their direct care via the WSIC system and their right to opt-out, which supports the common law requirement for implied consent to be informed.

A suite of information that provides detail about the use and sharing of patient information is publicly available on the WSIC website. This openness and transparency is an example of good practice and goes far towards supporting public awareness and fair processing. Some of the information however, is not clearly understandable for the public, such as the WSIC data flow map, WSIC data templates and Exclusion codes, which all include codes and acronyms that the public would not be able to interpret. Good practice would be further enhanced for example, by offering a glossary of terms or explanation/interpretation where things are not clear or would not be readily understood by a lay person.

Recommendation 1: Improve transparency and openness by reviewing the "Resources" information on the WSIC website designed to inform patients about the uses of their personal data, to ensure it is free from codes and acronyms that an ordinary person would not reasonable be expected to understand. Seek advice from the Lay Partners Forum to test all publications are clear, relevant and understandable.

Implied consent provides the lawful basis to flow personal confidential data from Provider Partner systems into the WSIC Integrated Care Record. A "permission to view" process is also in place whereby a patient is asked by front-line staff for permission to access the integrated care record, either by them or MDG team providing care. The GP record will be flagged with the appropriate clinical code to denote consent preferences expressed by the

[6] Independent Information Governance Review (Caldicott 2) Report Section 3.2 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf

[7] NHS Constitution Chapter 3a https://www.gov.uk/government/publications/the-nhs-constitution-for-england

[8] HSCIC Patients Objection management http://www.hscic.gov.uk/gpes/pom

[9] Service users –lay partners - are embedded within the programme's working groups with a 'Lay Partners Advisory Group' overseeing and challenging the programme's approach to engagement.

patient. The addition of an opt-out code prevents the data being extracted from the GP system into the WSIC system.

If patient choses to opt-out, it may compromise the provision and/or quality of direct care and it is therefore essential that this is explained so that the patient is aware of the consequence of their decision to their health and wellbeing in terms that are clear and understandable to ensure they have made an informed choice.

Where an adult refuses to consent to information being shared for their direct care, the GP must consider whether there is an overriding public interest that would justify information sharing (e.g. because there is a serious risk of harm) and take appropriate action to mitigate that risk, including explaining to the patient why their wishes cannot be respected.

National guidance should be followed when sharing information about patients who lack the capacity to make an informed choice.[10]

Recommendation 2: A documented procedure and script should be developed to guide front-line staff in how to obtain explicit patient consent and record opt-out codes into the GP system to ensure individual patient choice is upheld. The script should include appropriate wording to (a) explain choices available to them and what questions to ask to obtain explicit consent; and (b) explain the impact to their direct care if a patient dissents, including appropriate action to be taken when an opt-out decision has to be overridden.

The WSIC system needs to be capable of supporting individual preferences, which are far more complex than just "yes" and "no" to health and/or social care sharing data. For example, a patient may be happy for everything about them to be shared, but on the other end of the scale a patient may be happy for some but not all information to be shared, or want to prevent access to certain parts of their record to certain individuals (e.g. mental health with their GP). The current codes available offer a choice of:

- Refused consent for upload to local shared record (Read 93C1, CTV3 YaKRw);
- No consent for electronic record sharing (Read 9Nd1 CTV3 XaKII);
- Declined consent to share patient data with specified third party (Read 9NdH CTV3 XaNwT).

The use of the opt-out codes to prevent personal data from being used for indirect care purposes is confusing, wrongly assumed to only apply to care.data[11] and recently caused

[10] Various sources of guidance available – BMA Confidentiality and disclosure toolkit Card 7 http://bma.org.uk/practical-support-at-work/ethics/confidentiality-tool-kit; summarised in the February 2015 Parliamentary briefing Accessing and Sharing health records and patient confidentiality http://www.parliament.uk/briefing-papers/sn07103.pdf ; Mental Health Act 1983 Code of Practice (Chapter 10) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/396918/Code_of_Practice.pdf

[11] Care.data is a NHS England lead programme that involves the extract of patient information from GP systems by the HSCIC to be used for various analytical purposes not connected with direct care provision. The

concern when they were found to block data being used for health screening purposes[12]. In the absence of national guidance there is a risk of mismanaging communications and coding records; nevertheless the patient's right to object is something that cannot be ignored. Some of the personal data processed for commissioning purposes within the WSIC system relies on current s251 support[13], and it is a condition of that approval that patients are informed and given an opportunity to raise an objection. This right to object is obscure in the current patient information materials and further work needs to be undertaken to ensure this is clearly communicated. A WSIC Patient Consent Management Strategy should be developed to include procedural guidance and a script for GPs to ensure consistency in their approach to patients to confirm their explicit consent for sharing data for direct care and the use of Read/CTV3 codes in patient records to control the WSIC data flows for both direct and indirect care purposes.

Recommendation 3: Develop a WSIC Patient Consent Management Strategy and provide practical guidance for GPs in how to approach patients and manage their respective choices. Supporting communication materials for patients must clearly explain their NHS Constitution rights to object to their personal data being used for in-direct care purposes.

The level of sophistication for consent choices has not been explored, but the system needs to be able to offer patients a genuine choice and not compromise preferences by limiting their options to an all or nothing decision. It is assumed that the future-state system will include the technical capability to accommodate different levels of choice either through the Patient Knows Best (PKB) system or bespoke development, but the WSIC Patient Consent Strategy needs to inform the system specification.

Recommendation 4: The WSIC Patient Consent Strategy should identify all consent and opt-out requirements and ensure future-state systems can support various levels of patient choice.

The Governance Group is advised to review clause 3.17 in the Information Sharing Agreement, which says: "*Explicit consent shall not be sought before Personal Confidential Data is transferred into the Whole Systems Integrated Care Record, nor before Providers view reports about their own patients in line with the Case Finding Purpose. As the sharing is for Direct Care and Provider Partners shall have informed patients about the sharing in accordance with clauses 3.7 and 3.8, consent shall be implied*". This contradicts national (NHS England, HSCIC, Information Commissioner), BMA and GMC guidance that clearly state

programme is currently stalled and awaits the start-up of pathfinder projects to test communication materials and public opinion. http://www.england.nhs.uk/ourwork/tsd/care-data/

[12] Ref Paragraph Q697 http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/health-committee/handling-of-nhs-patient-data/oral/17740.html

[13] Secretary of State approval under the Health Service (Control of Patient Information) Regulations 2002 which allows the common law duty of confidentiality requirement for consent to be set aside to process personal data for a medical purpose other than the provision of direct care. http://www.hra.nhs.uk/about-the-hra/our-committees/section-251/what-is-section-251/

that the (risk stratification) process for case finding is not a direct care purpose (although it does lead to the provision of care).

Recommendation 5: The Governance Group should reconsider the lawful basis for processing patient confidential data for a "case finding purpose" as the reliance on implied consent does not appear to meet national or professional guidance. The outcome should inform the WSIC Patient Consent Strategy.

Conclusion:

- Implied consent to share personal confidential data for direct care purposes is supported by an active communications plan.
- A consent to view process will be in operation, supported by guidance
- The future-state WSIC system should have the capability to support various levels of patient choice to enable their control over information sharing decisions
- Explicit consent is required for the use of personal confidential data for indirect care purposes e.g. commissioning unless another legal base can be applied e.g. s251
- De-identified data will be used for indirect care purposes.
- Case finding definition of direct care purpose needs to be reviewed
- Communications materials should be reviewed to ensure they adequately explain patient opt-out choices for both direct care and indirect care purposes
- A WSIC Patient Consent Management Strategy should be developed with supporting guidance and communication materials to ensure the approach to consent and opt-out choices is managed consistently and supported by future-state systems.

Part 2 - Data Protection Act 1998

The DPA applies to any processing of personal data and is underpinned by eight principles.

The Act establishes a Data Controller as the person responsible for ensuring personal data is processed in compliance with the data protection principles.

A Data Controller can act alone, jointly or in common with other data controllers to determine the purposes for which and the manner in which personal data are processed.

The Act makes provision for a Data Controller to outsource their processing requirements to a "Data Processor". However, the Data Controller remains legally responsible for ensuring their processing activities comply with the data protection principles regardless as to whether that processing is done in-house or contracted out.

Data Controllers.

The Data Controllers responsible for the personal data in the WSIC system are:

- The GP Practices;
- Providers of health care services
- The Local Authority for adult social care services

(Collectively termed "Provider Partners)

The Data Processors are:

- NHS Brent Clinical Commissioning Group (Host)
- South East London Clinical Commissioning Group
- GP System suppliers
- GP system data extraction service suppliers

Each Provider Partner is the Data Controller in respect of the personal data that it holds and processes for their own purposes and as such acts alone.

The Provider Partners are data controllers acting in common when they provide personal data to be pooled in the Integrated Care Record and used for the common purpose of provision of direct care.

An Information Sharing Agreement is in place to provide a legally enforceable contract between the data controllers and NHS Brent CCG as their data processor. The ISA sets out the data controller accountability, responsibility and information governance terms and conditions for the use and sharing of personal data within the system and specifies their

instructions to the data processor. Each data controller must agree to and sign the ISA as a condition to joining the WSIC system.

A Whole Systems Information Sharing Agreement Governing Group (the "Governing Group"), whose membership comprises of Provider Partner representatives and lay partner (patient) representatives, oversees the sharing of information in accordance to the agreement.

Amendments to the Information Sharing Agreement have to go through the Governing Group and only agreed in consultation with and the consensus of all Provider Partners, which enables the Provider Partners to retain their individual control over the personal data they are responsible for.

The Information Sharing Agreement also governs any processing of de-identified data, although it ceases to be personal data subject to the data protection and confidentiality principles, enabling the Provider Partners to enforce the terms and conditions for use if necessary. This provides assurance that the data set won't be misused e.g. for unauthorised purposes, sold, exploited or used in any way beyond the reasonable expectations of the public (patients) that otherwise may cause enough concern for them to withhold their consent and risk harming the provision of care benefits the system is designed to support.

Conclusion

- Each Provider Partner is a Data Controller acting alone and responsible for the personal data of their respective patients
- The Provider Partners are Data Controllers acting in common when accessing personal data pooled in the WSIC system – but must adhere to the conditions set out in the legally binding Information Sharing Agreement.
- Brent CCG acts as Data Processor to the Data Controller Provider Partners and must only process personal data in accordance to the instructions set out in the Information Sharing Agreement.
- Each Data Controller is represented on the Governance Group and retains their independent decision making responsibility for changes made to the Information Sharing Agreement.
- The Information Sharing Agreement controls the way in which both personal confidential data and de-identified data can be used within the system.

First Principle

Personal data shall be processed fairly and lawfully and, in particularly, shall not be processed unless:-

a) At least one of the conditions in Schedule 2 is met, and

b) In the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met

Fair:

For processing of personal data to be fair, the data controller is required to ensure data subjects (patients) are informed about the way in which and the manner in which their data is used and not to use the data in any way that would be construed as unfair to the individual.

This is similar to the requirement for consent to be informed, however, the DPA Fair processing requirements apply to any processing of personal data, even where consent is not relied on to provide the lawful basis.

The requirement to inform is usually addressed by issuing "Fair Processing notices" (FPNs), and the publication and distribution of information to explain to the local population about the use of their personal and sensitive personal information within the WSIC system and their rights to object discussed in the previous section meets this obligation.

It is however necessary to emphasise that the publication and distribution of information only satisfies one part of the DPA first principle.

The responsibility for the distribution of the fair processing information lies with each individual Provider Partner as the Data Controller. Section 3.7 – 3.17 of the Information Sharing Agreement sets out the specific requirements to meet this data protection condition.

Processing personal data outside of the terms and conditions specified in the FPN and Information Sharing Agreement should be construed as being as unfair to the individual, unless separate action has been taken by the responsible Data Controller to provide additional information to ensure that processing is fair.

Any failure of the Data Controller to fulfil these obligations risks the integrity of the whole WSIC system therefore (in addition to a DPA condition) fair processing is a condition of the Information Sharing Agreement and the Governing Group should ensure this requirement is being met to a consistent standard and enforce the terms and conditions against any Provider Partner failing in this duty.

The Fair Processing Notices inform the data subjects (patients) of their right to object to the data processing. It is the responsibility of the respective Data Controllers to:

- Take steps to actively communicate the information to ensure it reaches the vast majority of their patients, including hard to reach patients; and
- Allow a reasonable period of time for patients to exercise this right before data is uploaded to the WSIC system.

It would be unfair (and therefore unlawful) to extract data from Provider Partner systems in advance of informing patents. It is assumed that this will be scheduled into the project plan when data starts to be extracted to populate the WSIC system therefore implementation

needs to be supported by a communications plan that clearly sets out a timetable for data controllers to follow.

Recommendation 6: Develop a communications plan to support the GP Practice Data Controllers in their duties to ensure their registered patient population are adequately informed and have a reasonable period of time in which to register any objections before data is extracted for the WSIC system.

The Information Sharing Agreement (section 8.1) explains the intention to hide data so as to make it inaccessible should a patient express an objection after data has been uploaded into the WSIC system. The hidden data is held for a period of six months "in case the patient changes their mind". The Governing Group are advised to reconsider this arrangement. If a patient objects after their data has been uploaded, then their wishes should be respected and the data deleted from the system at the next extract. If however the decision is to hold data, then this should be explained to the individual as they may not expect that to happen (their expectation is that having said no, their data will not flow into the WSIC system) and they should be allowed to raise a further objection to the data being held in this way. , otherwise it could be construed as unfair.

Recommendation 7: The Governing Group should review the Information Sharing Agreement section 8 to either (a) permanently delete data held in the WSIC when a patient registers an objection, or (b) inform the patient of the intention to hold hidden data for a period of six months and allow them to raise a further objection if they do not they agree to that.

Conclusion

- Section 3.7 – 3.17 sets out the fair processing requirements that each data controller is responsible for executing.
- A reasonable period of time should be allowed for patients to register an objection after fair processing information has been communicated and before data is extracted from GP systems into the WSIC system.
- A communications plan to support those requirements and set out a timetable for completion should be developed (recommendation 6).
- The Governing Group should review section 8 of the Information Sharing Agreement to mitigate the risk of unfair processing of data held after a patient has chosen to opt-out (recommendation 7)

Lawful:

Lawful data processing requires the Data Controller to ensure that they act intra vires by:

- Having the legal remit or power to process personal data in the way in which they intend to use it; and
- Ensuring that the processing meets common law and relevant statutory requirements.

Public sector organisations will derive their lawful powers through legislation that has set them up and establishes their remit. Recent changes to the National Health Act 2006 implemented by the Health and Social Care Act 2012 and the enactment of the Care Act 2012 in April 2015 establish the legal duties upon health organisations and local authorities work together to integrate care[14]. Independent and 3rd sector service providers will have implied powers through the contract arrangements made with the public body commissioners.

The HSCIC's legal powers to collect, analyse and disseminate national health and social care data are set out in the Health and Social Care Act 2012. These powers can only be activated when the HSCIC is directed to establish information systems by the Secretary of State for Health or by NHS England, or requested to do so by other bodies. The Act also places restrictions on the way in which the HSCIC can disclose or publish data[15].
NHS England have issued Directions to the HSCIC[16] to establish and operate systems for the collection and analysis of local commissioning data sets; and/or as requested by a Relevant body[17] party to a commissioning contract with a health service provider. Directions for the collection and analysis of social care data have not been issued.

The South London DSCRO provides data services for the NWL WSIC system and operates under the delegated powers of the HSCIC.

The WSIC data flows diagram illustrates data flowing into and through the WSIC system.

Stage 1. NHSE Directions provide the lawful basis to flow SUS, PbR, Community MDS and Mental Health MDS into the DSCRO. Primary Care System data – EMIS and TPP SystmOne flows on an implied consent basis for a direct care purpose. It is assumed this is supported by a documented agreement with the DSCRO.

Stage 2. GP system data cannot be linked to other data to be used for commissioning purposes under implied patient consent therefore another legal basis must be sought. An application for s251 support was submitted in January 2015. Approval has been granted, but this is subject to certain conditions including

[14] Sections 13N and 14Z1 of the National Health Service Act 2006 as inserted by the Health and Social Care Act 2012; and sections 3, 6 & 7 of the Care Act 2014.
[15] http://www.legislation.gov.uk/ukpga/2012/7/contents/enacted Health and Social Care Act 2012 Part 9 Chapter 2
[16] NHS England The Health and Social Care Information Centre (Establishment of Information Systems for NHS Services: Data Services for Commissioners) Directions 2013.
[17] Ibid (17) Part 9 Chapter 2 section 255 (1) (2) and (4)

a requirement to inform all patients of their right to object. This is under consideration by the Governing Group.

Stage 3. The DSCRO transfers clear data (collected at Stage 1) into the South East Commissioning Support Unit (SE CSU) for translation into viewing screens in the WSIC Integrated Care Record. It is assumed this processing is done under the implied consent for direct care basis, however, consent would not override the conditions for processing SUS and commissioning data sets set out in the NHS England Directions and Data Sharing Contract and Data Sharing Agreement between the HSCIC and CSU. SUS and commissioning data sets flow from the DSCRO into the CSU (Stage 1 Accredited Safe Haven (ASH)) [18] under the legal basis provided by s251 approvals. In accordance with the DS Contract and Agreement, this data should not be "combined with other data or must not be used or manipulated in any way that re-identifies and individual" (contract clause 4.4); and "data must not be shared" (7.1.4 of the Agreement) unless agreed by the HSCIC. This agreement needs to be more transparent.

New Regulations are to be introduced which establish the Stage 1 ASH's legal basis to process health and care information. Subject to changes following a public consultation, the draft Regulations included legal powers for an ASH to provide "those responsible for providing care to an individual with information that might inform or support that care"[19]. It is assumed this clause will be established in the final version, in which case the Regulations will establish the lawful basis to support this data flow. The Governing Group are therefore advised to review this data flow when the Regulations are implemented to ensure it is supported by a continuing legal basis.

Stage 4: GP systems data flowing into the Whole Systems Care Records Dashboard (Pseudo data) and Demo Tableau (de-identified data) as illustrated in the data flow diagram is subject to the outcome of the Governing Group's s251 decision to support linkage. The planned flow of social care data will need to be underpinned by a legal basis and it is assumed this will be met via one of several options available provided by either section 255 of the Health and Social Care Act 2012 (Request) or incoming Regulations.

In all cases, there is a requirement to ensure that patients are informed of their NHS Constitution rights to object to the processing of personal data.

[18] http://www.hscic.gov.uk/article/3697/Register-of-Stage-One-Accredited-Safe-Havens

[19] Protecting Health and Care Information – Department of Health consultation on proposals to introduce new Regulations Section 26 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/323967/Consultation_document.pdf

Recommendation 8: The Governing Group are advised to be aware of the conditions for processing personal data and regularly review the WSIC data flows against changing circumstances to ensure there is a current and future legal basis to support the usage and proposed usage of data. It is also important to be aware of the requirement to inform patients about their right to object to secure any legal basis relied upon.

In addition to the first principle requirements for the processing of personal data to be both fair and lawful, the processing also has to meet certain conditions set out in Schedule 2 for personal data and both a Schedule 2 and a Schedule 3 condition if the data is sensitive personal data.

Schedule 2 condition:

A Schedule Two condition has to be met to enable personal data to be processed lawfully.

Health and Local Authority social care services:

Schedule 2 (5) (c) "The processing is necessary for the exercise of any function of the Crown, a minister of the Crown or a government department.

Independent service providers:

Schedule 2 (5) (d) "for the exercise of any other function of a public nature exercised in the public interest by any person".[20]

Schedule 3 condition:

Both a Schedule 2 condition and a Schedule 3 condition must be met when processing "sensitive personal data"

Sensitive personal data is defined in section 2 of the Data Protection Act 1998 and includes categories of data processed within the WSIC such as physical and mental health conditions and ethnicity.[21]

Health service providers:

[20] Independent service providers commissioned to provide health or social care services will, through the terms and conditions of their contract, be required to act in accordance with all laws and principles that a public authority will be required to act through legislation. It is in the public interest that any provider providing services of a public nature are bound by the exact same terms and conditions as the public authority contracting them.

[21] Data Protection Act 1998 section 2
http://www.legislation.gov.uk/ukpga/1998/29/pdfs/ukpga_19980029_en.pdf

Schedule 3 (8) (1) "The processing is necessary for a medical purpose undertaken by:

a) a health professional, or
b) a person who in the circumstances owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

(2) In this paragraph "medical purposes" includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

Local Authority care service providers:

Schedule 3 (7) (1) (c) "The processing is necessary for the exercise of any function of the Crown, a minister of the Crown or a government department".

Conclusion:

- Each Provider Partner is a Data Controller and individually legally responsible for ensuring compliance with the data protection principles.
- The Governing Group are advised to review the lawful basis for processing, particularly in line with imminent changes to existing arrangements and incoming Regulations.
- A decision about accepting s251 approval with conditions to link GP data is awaited.
- Subject to the recommendations within this section the DPA first principle requirements are met

Second Principle

Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes

Each Provider Partner as a Data Controller is required to have notified the Information Commissioner of their data processing activities, which are entered on the publicly available register. It is assumed this is already in place.

The notification serves as a limitation by ensuring processing does not extend beyond the limits of the registered purposes otherwise the processing would be deemed as unlawful. There is nothing to suggest through this assessment that this principle is not being met

Conclusion:

- The Information Sharing Agreement requires each Provider Partner to have appropriately registered their data processing activities with the Information Commissioner. A failure to do so would invalidate their agreement and constitute unlawful processing.
- The DPA second principle is met

Third principle

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed

The NWL Whole Systems data template[22] lists the various lines of data available in Provider Partner systems agreed for sharing. Only codified data will be extracted from Provider Partner systems.
Data feeds from the Provider Partner systems are translated into one or more viewing screens on the software portal.

Working groups were set up to scope the data requirements that reflected local need and the Governing Group signed the resulting data templates.
Various exclusion codes will be used to prevent certain data from being uploaded into the WSIC e.g. where statute restricts the use and sharing of highly sensitive clinical data items such as sexually transmitted diseases, human fertilisation and embryology etc.

The data sets contain a variety of administrative and clinical data, not all of which (the majority of which) could be justified as being necessary for a direct care purpose. For example, continuing care and social care datasets are mainly based on costs and funding and contain no clinical data; SUS (Secondary Use Services) data is expressly for purposes other than direct care[23]

[22] NWL Whole Systems Data Template September 2014
http://integration.healthiernorthwestlondon.nhs.uk/Images/upload/2014-09-26%20WSIC%20Data%20Templates%20Reference%20Document%20V2.pdf
[23] http://www.hscic.gov.uk/sus

The WSIC data flow diagram was used to assess the lawfulness of the transfer of data for the first DPA principle. There is not enough information on the flow diagram to study the transfer of data in the detail needed to assess compliance and/or risks with this third principle. In the absence of further information, it is not clear why certain data items are included in the data schedules where the purpose is for direct care and data flows under an implied consent assumption. Whilst the intention is to only use de-identified for indirect care purposes, there has to be a legal basis supporting that data flow into the system in the first place in order for it to be stripped of identifying elements for further use; and patients have a right to know and to object to this use of their data.

The purpose for using the data has to be clear to be able to judge what data is needed in terms of proportionality, relevance and necessity[24] to meet that purpose and that level of understanding is essential in order to accurately complete this part of the assessment.

If the purpose of the WSIC IT system is for supporting the delivery of direct care to an individual, then the data fields containing administrative and finance based data may not be necessary. The Royal College of Physicians Standard for the Clinical Structure and Content of Patient Records (July 2013) provides guidance on the clinical record headings and a description of the information that should be recorded under each heading, and should be used to inform the review. [25]

If, however, the purpose of the system is to support health and social care services to coordinate the delivery of health and social care, then some of the clinical data elements listed may be excessive (in addition to invalidating the reliance on implied consent).

It is therefore advisable to consider the minimum data sets in terms of relevance and proportionality for the clear and specified purposes.

It is essential that this is completed to inform the drafting of the system specification prior to starting the procurement stage and development of the system.

Recommendation 9: The clear purpose for the WSIC system should be determined, following which the data items in the Data Schedules should be reviewed to ensure they are relevant, proportional and necessary to meet that purpose. The RCP Guidance should be followed to determine the content of the Integrated Care Record.

Conclusion:

It is not possible to complete a full assessment against the third principle requirement until:

- The purpose(s) of the WSIC system is clearly defined
- Data items to meet that purpose/those purposes are identified and justified as being proportionate and necessary to meet that purpose.
- Clarity is essential to inform the system specification and the public
- RCP guidance should be followed to inform the content of the Integrated Care Record

24 A
th
25
pa
W

Fourth principle

Personal data shall be accurate and, where necessary, kept up to date

Each data controller is responsible for ensuring the data in their respective systems is kept accurate and up-to-date. It is assumed that this is achieved through various measures such as validation of data against national data systems held by the HSCIC e.g. PDS and by regular checks made with the patient at points of contact e.g. when they attend a clinic etc.

Consideration must be given to designing a whole systems procedure to deal with data feeding into the integrated care record from two or more systems does not match up. A central point of contact (clearing house) for dealing with inaccuracies to identify the single point of truth and notify the relevant Provider Partners in order to ensure the data is updated in the correct sequence in time for the next data extract is recommended. Documented guidance to support front line staff, including clear responsibilities for ensuring the relevant Provider Partner is notified and source data is corrected to avoid the error repeating in subsequent data extracts.

The future-state system will extract data on a daily basis which will capture changes made to the source data and improve accuracy and reliability of data in the Integrated Care Record.

Recommendation 10: A whole systems procedure for managing inaccuracies in the Integrated Care Record focussed around a central point of contact to support front line staff in the reporting and correction of data should be established. The procedure should be documented to identify responsibilities and provide clear instruction to staff to ensure a consistent approach.

The Integrated Care Record is a read only system to be used as a point of reference in a direct care setting. Clinical decisions made at that time are recorded in the relevant Provider Partner's system and the subsequent flow into the Care Record is dependent upon the next data extract. Daily extracts will keep the record more up-to-date, however, a true digital integrated record must be capable of real-time updates via write-back capability automatically recording the date, time and the identity of the person making the entry. This requirement should be included in the system specification to ensure the future-state system records clinical information in a way that can be shared and re-used safely in a paperless environment.

Recommendation 11: The system specification should include future-state capability to ensure a full digital integrated care record that supports real time entry of clinical information.

Conclusion

Accuracy of data within the system can be improved by:

- A coordinated procedure to deal with inaccuracies in the data held in the WSIC record should be established.
- The procedure should be communicated to all Provider Partners and included in the Information Sharing Agreement
- A daily extract of source data
- Read and write functionality to support direct care

Fifth Principle

Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purposes or those purposes

The WSIC Data Retention policy is set out in section 8 of the Information Sharing Agreement.

Each data controller operates their own separate retention and disposal schedules for source data determined by the NHS Records Management Code of Practice[26].

Data held in the WSIC system that has become redundant (for various reasons) that had previously been used for that patient's direct care will also be retained in accordance with the NHS guidance.

It is proposed that one data extract will overwrite data held in the system from the previous data extract.

The clinical governance of both current and legacy data must be maintained to ensure information used at the point of direct care to inform a clinical decision can be identified and reproduced to legal admissibility standards as evidence for medico-legal purposes[27].

Whilst anonymised data is excluded from the DPA principles, there may still be NHS retention periods that apply, therefore all data must be included in the WSIC policy.

Recommendation 12: Data should be retained in accordance with the NHS Records Management Code of Practice in a format that enables it to be reproduced in accordance with recognised medico-legal standards for the lifetime of that record. Assurances that this requirement will be included in future state systems is essential and therefore must be included in system specifications.

[26] Records Management NHS Code of Practice http://systems.hscic.gov.uk/infogov/records

[27] Cabinet Office guidance http://www.thecabinetoffice.co.uk/page28.html

Conclusion

- WSIC data retention and disposal policies have been determined and meet NHS Guidance.
- Future state clinical governance requirements must be included in the system specification
- Data must be retained in a way that ensures reproduction meets recognised legal admissibility standards

Sixth principle

Personal data shall be processed in accordance with the rights of data subjects under this Act

Data subjects have the right to;-

- Be informed about how their person information will be processed;
- Have access to a copy of their personal information held by data controllers;
- To have inaccurate information corrected, blocked or erased;
- Be informed of who has accessed to their records; and
- object to processing that is likely to cause them damage or distress

Each data controller has a system in place to subject access requests (SAR). Individuals have to go through a bureaucratic system when applying for access, which is subject to a fee determined by the data controller that should not exceed the prescribed £50 maximum (most organisation have a flat rate of £50). The agreed system for responding to SARs is to refer patients to the relevant data controller.

This needs to be reconsidered. Patients should be provided with access to their Integrated Care Record held in the WSIC system. If it is possible for a health or care professional to have access to a shared record, then there is no reason to refuse the patient access to the same information. It is an accessible record as defined in the DPA and refusal to a request for access would be an unlawful act by not meeting the sixth data protection principle. Denial of access could be interpreted as a breach of Article 8 of the Human Rights Act 1998.

Recommendation 13: The Governing Group are advised to review the Information Sharing Agreement section 6.5 decision on arrangements for dealing with subject access requests. The Integrated Care Record held in the WSIC system is an accessible record and patients have a legal right to be provided with a copy upon request.

Information recorded in the audit trail will enable a list of users who have accessed the record to be produced and provided to the patient upon request. This should be included in the system specification.

Other data subject rights are addressed by compliance with the first and fourth principles.

The system will ultimately provide an individual with access to their own record and it is assumed that this will reduce the number of subject access requests.

Conclusion

- A procedure for dealing with subject access requests for information held in the WSIC Integrated Care Record WSIC should be established.
- The system must include the technical ability to identify all users who have access an individual's record and made available to that individual upon request
- Providing an individual with direct access to the system will meet the sixth principle requirements in the future.
- Although not certain, it is assumed this will reduce the amount of subject access requests

Seventh principle

Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss of destruction of, or damage to, personal data

It is assumed that each data controller has robust technical and organisational measures in place to meet the information security requirements of the seventh principle. This can be measured by achievement of the mandated level two standards set out in the Department of Health's Information Governance Toolkit and satisfactory compliance is a condition of the Information Sharing Agreement.

It is assumed that the process of extraction from the Provider Partner's systems into the WSIC system will be secure and meets Department of Health standards and legal requirements of this principle.

Documented policies and procedures that support the information security management system, such as agreed role based access levels, security of mobile data etc. need to be developed for the WSIC system, agreed and signed by each Provider Partner and form part of the suite of Information Sharing Agreement materials.

The seventh principle also contains certain provisions that apply when a Data Controller contracts a Data Processor to process personal data on their behalf:

Seventh principle Schedule 1 Part II

> *Section 11*
> *Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller must in order to comply with the seventh principle—*
> *choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the processing to be carried out, and take reasonable steps to ensure compliance with those measures.*
>
> *Section 12*
> *Where processing of personal data is carried out by a data processor on behalf of a data controller, the data controller is not to be regarded as complying with the seventh principle unless –*
> - *the processing is carried out under a contract –*
> - *which is made or evidenced in writing, and*
> - *under which the data processor is to act only on instructions from the data controller, and*
> - *the contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle.*

It is assumed that the technical specification for the WSIC system will include all applicable information security requirements to prescribed industry standards, including penetration testing, business continuity and disaster recovery plans, and that potential system suppliers can provide guarantees that such measures will be in place.

The Information Sharing Agreement is legally binding and, in addition to establishing the principles underpinning the data sharing between the data controllers, it provides instructions to Brent CCG who acts as their data processor.

Each data controller must have a written contract with each data processor supporting the WSIC system as a condition of the seventh data protection principle. The Act is specific in that a data controller will not be considered to have complied with the seventh principle if this condition is not met[28].

This can be achieved in various ways, for example, Brent CCG is authorised to sub-contract with other data processors and each data controller is listed on that contract; by assigning one data controller to lead on data processor contract arrangements on behalf of the other data controllers; or each data controller establishes their own contract requirements with each data processor. In all cases it is essential that there is a clear auditable trail to evidence the connection to a written contract between individual data controllers and the respective data processors and ensuring those data controllers are included in the decisions making process concerning those contracts.

[28] DPA Schedule I Part II chapter 12 (a) and (b). It is noted that non-compliance with this condition has been a cause for the Information Commissioner to impose monetary penalties on NHS data controllers.

The required technical and operational security measures must be included in the written contract between the data controllers and the data processors with appropriate legal sanctions in place for breach of contract. The Information Sharing Agreement, which acts as a legally binding agreement between the data controllers and Brent CCG as the data processor, specifies Information Governance Toolkit requirements, which include the industry standards for information security, however, the DPA states (at 12 (b)) "the contract requires the data processor to comply with obligations equivalent to those imposed on a data controller by the seventh principle", which is not made evidently clear in the Agreement. In addition, the Agreement identifies Brent CCG as the "Host" and data processor for the system and controls sub-contracting arrangements (to those listed) instructing (amongst other things) the technical and organisational measures that need to be in place as a condition (at 9.7.4), but it is not clear what contracts are in place, who the contracts are between or other governance arrangements such as accountability and responsibility for auditing and ensuring compliance etc.

Assurances were provided to the reviewer that written contracts are in place, but these were not available or evident for the PIA process and therefore need to be more visible.

Recommendation 14: The Governing Group should review the existing data controller/data processor contracts to ensure they (a) clearly identify those data controllers the contract applies to and (b) clearly include the DPA seventh principle conditions for information security. The contracts should be subsequently reviewed on an annual basis (or earlier if circumstances dictate)

Conclusion:

- An Information Sharing Agreement between the data controllers and Brent CCG as the Host and data processor specifies the information security requirements for the system and includes instructions for processing.
- Contract arrangements with the sub-contracted data processors including assurances and management of those contracts is not clear and need to be made more visible
- The Governance Group should ensure all contracts contain the appropriate governance arrangements and clearly apply to each data controller party to that contract
- An annual review process should be introduced.

Eighth principle

Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

Assurances have been provided that no data will be held or processed outside of the UK or the EEA. This however will need to be stated as a requirement in the system specification and confirmed by the system supplier as part of the procurement process.

Conclusion

The eight principle is not relevant to the WSIC system

Section 3 - The Human Rights Act 1998

The Human Rights Act (HRA) incorporates the European Convention on Human Rights (ECHR) into English law. It is unlawful for a public body to act in a way that is incompatible with the HRA.

Article 8(1) states "Everyone has the right to respect for his private and family life, his home and his correspondence."

This is not an absolute right and is qualified by Article 8(2) which states "there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others".[29]

A public body can only interfere with this Article 8 right if it is proportionate and justified as necessary in the interest of the wider community or to protect the rights of others.

Any disclosure of confidential information about a patient to another person or body is an interference with an individual's private life. To do so without consent is a violation unless the public body could justify that it was proportionate and necessary in the interest of the wider community or to protect the rights of others.

Compliance with the common law duty of confidence and the DPA will usually mean Article 8 requirements are also met.

The recommendations made in this report highlight some areas of privacy risk and provide advice on remedial actions.

The biggest risk identified that applies to all three areas of statute, is the approach to consent and in particular the absence of information to clearly explain to patients their right to object to their personal data flowing into the system when the purpose of that data flow cannot be justified as a direct care basis.

[29] http://www.legislation.gov.uk/ukpga/1998/42/schedule/1/part/I/chapter/7

Informing individuals about this right is a specific condition of the recent outcome of the s251 application for support to link GP data with other commissioning data. It has been a condition of existing s251 approvals that are in place to support the CCGs (or CSUs) use of SUS, PbR and commissioning data that has not already been met. It is likely that it will be a condition of the incoming Regulations that establish ASHs on a statutory basis.

This requirement is already listed in the previous recommendations therefore it is highlighted as important but not reiterated here.

Recommendation 15: This PIA is a progressive living document and should be reviewed on a regular basis by the Governing Group on a regular basis (every 3 months initially moving towards an annual review when stable) to ensure remedial actions are taken as recommended and the outcomes and risks are considered in line with legal changes and developing guidance.

Glossary		
Term	**Alternative terms**	**Definition**
Aggregated data/information	Statistical data;	Statistical data about several individuals that has been combined to show general trends and values without (a) identifying those individuals within the data, and (b) where the identity of those individuals cannot be determined.
Anonymised data/information	De-identified data; aggregated data	Data that has been converted into a form that does not identify an individual or individuals within the data set and where identification is unlikely to take place. The following standards apply: 1. Information Standards Board Anonymisation Standard www.isb.nhs.uk/library/standard/128 2. Information Commissioner Anonymisation: managing data protection risk code of practice https://ico.org.uk/for-organisations/guide-to-data-protection/anonymisation/
Anonymised data for publication	Effectively anonymised data	Anonymised in accordance with the above standards and deemed to have a low risk of re-identification enabling publication.
Confidential data/information	Identifiable data/information; personal information; personal confidential information	Information which is in a form that identifies an individual to whom the information relates or enables the identity of an individual to be ascertained, or any other information in respect of which the person who holds it owes an obligation of confidence.
Consent		Consent is the approval or agreement for something to happen after consideration. For consent to be legally valid, the individual must be informed, must have the capacity to make the decision in question and must give consent voluntarily. This means individuals should know and understand how their information is to be used and shared (there should be 'no surprises') and they should understand the implications of their decision, particularly where refusing to allow information to be shared is likely to affect the care they receive. This applies to both explicit and implied consent. The Mental Capacity Act 2005 Code of Practice should be consulted with regards to decisions about capacity and competence. (*Source HSCIC Guide to confidentiality – references*)
Data Controller		Data Protection Act 1998 Part 1 section 1 definition. A person who (either alone, or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data is processed.
Data Processor		Data Protection Act 1998 Part 1 section 1 definition: In relation to personal data means any person (other than an employee of the data controller) who processes the data on behalf of a data controller
Data Subject		A Data Protection Act 1998 Part 1 section 1 definition: An individual who is the subject of personal data.

De-identified data	De-identified data for limited use; Pseudonymised data; Anonymised data	Information which identifies an individual has been removed. Only effectively anonymised data falls out of the scope of the privacy laws.
De-identified data for limited access	Pseudonymised data (N.B. the term "weakly pseudonymised data" should not be used	Data that has undergone a process of anonymisation but is deemed to have a high-risk of re-identification if published but a low risk if held in a secure environment with controls in place (e.g. contractual, legal) to prevent re-identification
Explicit consent		Explicit consent is unmistakable. It can be given in writing or verbally, or conveyed through another form of communication such as signing. A patient may have capacity to give consent, but may not be able to write or speak. Explicit consent is required when sharing information with staff who are not part of the team caring for the individual. It may also be required for a use other than that for which the information was originally collected, or when sharing is not related to an individual's direct health and social care. (*Source HSCIC Guide to confidentiality – references*)
Identifier		An item of data, which by itself or in combination with other identifiers enables an individual to be identified. Examples of identifiers are provided in the HSCIC Confidentiality Guide (References) (page 48) http://www.hscic.gov.uk/media/12823/Confidentiality-guide-References/pdf/confidentiality-guide-references.pdf
Implied consent		Implied consent is applicable only within the context of direct care of individuals. It refers to instances where the consent of the individual patient can be implied without having to make any positive action, such as giving their verbal agreement for a specific aspect of sharing information to proceed (Etc.) (*Source HSCIC Guide to Confidentiality – references*).
Linkage		The merging of data/information from two or more sources with the object of consolidating facts concerning an individual or event that are not available in a separate record.
Personal Confidential Data	"PCD", confidential data/information, identifiable data, personal data	A term established in the Independent Information Governance Review 2012 (Caldicott2) and now in common use within the health and social care sectors. PCD is personal information about identified or identifiable individual(s), which should be kept private or secret and includes the DPA definitions of personal and sensitive personal data about deceased or living individuals. "Confidential" is information which is either "given in confidence" or "that which is owed a duty of confidence".
Personal data		Data Protection Act 1998 Part 1 section 1 definition: "Personal data" means data which relate to a living individual who can be (a) identified from those data , or (b) from those data and any other information which is in the possession of, or likely to come into the possession of the data controller (etc).
Pseudonymised data	De-identified data; de-identified data for limited access	Personal data that has been through a process of removing identifiers and replacing them with a coded reference or pseudonym enabling that data to be associated with the

		individual but without that individuals "real world" identity being known. Pseudonymisation is not a method of anonymisation - EU Article 29 Data Protection Working Party Opinion 5/2014.
Re-identification	De-anonymisation	The process of analysing or combining (linking) data with other data with the result that the individual becomes identifiable.
Sensitive personal data		Data Protection Act 1998 Part 1 section 2 definition: Personal data consisting of information as to the racial or ethnic origin of the data subject; political opinion; religious beliefs or beliefs of a similar nature; membership of a trade union; physical or mental health; sexual life; legal proceedings against the individual or allegations of offences committed.

NB Definitions taken from the Health and Social Care Information Centre (HSCIC) confidentiality guidance and codes of practice and from the Data Protection Act 1998.

Health and Social Care Information Centre: A guide to confidentiality in health and social care:

http://www.hscic.gov.uk/3444

Data Protection Act 1998

http://www.legislation.gov.uk/ukpga/1998/29/contents