Reference Number 000…

Date

Digital
North West London

Data Management: Change Request Form

Introduction

In order to assist with this review those providers partner and named data processors using Data Sets supplied by the respective provider partner Business Intelligence Functions, there is a need to submit the attached form. The form sets out a series of questions to help determine whether the information flow can continue in its current form.

When completing the information flow request form, please review it before submission, to ensure it is up to date and all relevant information about the flow has been supplied.

(For further details, See Appendix B, Outline Process)

Annex A - Information Flow Review Form

1.0 What type of information is being requested? (See Appendix A)

1	**Personal Data**	
2	**Sensitive Personal Data**	
3	**Patient Identifiable Data**	
4	**Personal Confidential Data**	
5	**Patient Level Data**	

Escalated to Governance Group	**Date Proposed**
Yes	
No	
To be noted at meeting	

2.0 Which organisation and function are you submitting this form on behalf of?

Organisation	
Function	
Department	

3.0 Who is the contact point for the Information Flow? (This is a staff member who can provide additional details and answer questions, in IG terms the Information Asset Administrator)

Name	
Post	
Contact Email	
Contact	
Date of Request	
System Requested	WSIC Dashboards / Care Information Exchange

Digital
North West London

Data Management: Change Request Form

4.0 What impact does the information flow have?

Which of the following categories does the data flow fall into? (select one)

1	Must be kept operational, with no outage	
2	Must be operational within 24 hours	
3	Must be operational within 3 days	
4	Must be operational within 7 days	
5	Can be operational after 7 days	

Does the flow pose any risks on the following issues?

Clinical		**Business**		**Financial**		**Operational**	

Outline the business impact and timescales associated with the use of information flows? *(For example, the data set is used to update the virtual ward for Borough NAME and is updated on a daily basis)*

5.0 Tell us about the information flow:

What type of flow is it?

This would be reference to a relevant act or explanation of how the processing supports direct healthcare or healthcare management, see below.

For example, does the processing support any of the following?:

1	Explicit consent of the person (Sch. 3[1]) DPA 1998	
2	NHS Act 2006 s.251 accepted flow (Sch. 3[3]) DPA 1998	
3	By Enactment (Sch. 3[7]) DPA 1998, includes HSCA 2012 enabled flows (from s.250 to s.277)	
4	Medical purpose (Sch. 3[8]) DPA 1998	✓
5	Pseudonymised – weak identifier required, linked to HSCA 2012 enabled flows (from s.250 to s.277)	
6	Pseudonymised – weak identifier required, but you have no capacity to revert it to PCD	
7	Anonymous (aggregated data with **NO** PCD)	

Where does the information come from?

Organisation	
Function	

What information is being shared? *(Provide a broad description of the information being received)*

Digital
North West London

Data Management: Change Request Form

If you have an example Data Set (one which shows the types of information but example contents or descriptions) please provide it along with this form.

What do you use the information flow for? *(Provide a broad description of the purposes you use the information for)*

Why is this information essential for the specified purpose(s)?

Have you reviewed the use of information and (a) identified the minimum information required to fulfil the purpose or (b) considered the use of pseudonymised or de-identified data? (*Tell us why you have to use identifiable data and the data set you intend to use)*

6.0 Legal Basis for Processing Identifiable Data

You must have a lawful and fair basis to process Patient Identifiable Data (PID) or Patient Confidential Data (PCD). See Annex B for the definitions of Data.

Lawful Basis Under Schedule 2 of the Data Protection Act

Click this link http://www.legislation.gov.uk/ukpga/1998/29/schedule/2 for the Act

Lawful Basis Under Schedule 3 of the Data Protection Act, this schedule is relevant for sensitive data which includes health and sexual life or history

Click this link http://www.legislation.gov.uk/ukpga/1998/29/schedule/3 for the Act

7.0 Safe Haven and Access Controls

Safe Haven and Access Controls are requirement to process data lawfully. Can you provide a brief description of how the data is protected and how access is restricted:

Access to the Data is limited to *(Describe who has access to the information)*

We control access to the patient data in the following ways *(Describe how you control access to the information)*

Digital
North West London

Data Management: Change Request Form

Information is stored in the following locations and with the following security controls/mechanisms (?) *(Describe where the information is stored and how security is maintained, for example password, restricted access, partitioned shared drive)*

How long do you keep copies of the information?

All done? Submit your form to BRECCG.NWLWholeSystems-ISA@nhs.net along with the relevant Information Flow Map where appropriate.

Digital
North West London

Data Management: Change Request Form

Annex C – Comments & Approval

Approved	Comment	Date Actioned
Yes		
No		
Other		

Name	
Job Title	
Organisation	
Contact Email	
Date	

Digital
North West London

Data Management: Change Request Form

Appendix A- Definition

Health Professional	**Health Professional** is defined under the DPA 1998, and generally refers to a practitioner registered with one of the relevant professional bodies, see for more information: Data Protection Act 1998, 1998 c. 29, Part VI, General, Section 69, see link http://www.legislation.gov.uk/ukpga/1998/29/section/69
Personal Data	**Personal Data** means data related to a living individual, within the health service We must be mindful of deceased patients due to the duty of confidentiality which extends beyond dead. It allows them to be identified from the data (or with data that may come into their possession) As defined by the Data Protection Act at http://www.legislation.gov.uk/ukpga/1998/29/section/1
Sensitive Personal Data	**Sensitive Personal Data** requires additional conditions for processing and consists of 8 categories, the following three are the most relevant (a) racial or ethnic origin (e) physical or mental health or condition (f) sexual life As defined by the Data Protection Act athttp://www.legislation.gov.uk/ukpga/1998/29/section/2
Patient Identifiable Data	**Patient Identifiable Data (PID)** is information about patients from which they can be identified.
Personal Confidential Data	**Personal Confidential Data (PCD)** is information about patients both living and dead which must be managed to a standard of confidentiality, in line with the BMA and GMC expectations. The formal definition will be provided in the Caldicott 2 Review report released on 17 April 2013
Patient Level Data	**Patient Level Data** is data about individual patients that does not allow the patient to be identified by providing (a) a restricted data set or (b) de-identifying information
De-identification	**De-identification** is a process that removes identifiers to data, in-order to enable its wider use. For example, for secondary use purposes not directly related to healthcare or its management. See Pseudonymisation and Aggregation.
Legitimate Relationships	**Legitimate Relationship** is a term used to describe a basis for access to PID or PCD, due to it being passed from clinical to clinical staff/organisations for direct healthcare, or by the administrative team supporting access to healthcare.

Digital
North West London

Data Management: Change Request Form

Appendix B- Outline Process

A – Review your information flows for key Data Sets. Data Sets are sets of data (rather than individual requests like IFR or Continuing Care), such as the SLAM data from an Acute provider. Identify the business critical requests first, i.e. those with an immediate impact on clinical care, financial returns (related to FY 2012/13 for example) or wider business.

B – You will then need to complete the attached form. This asks for a contact point, which is a staff member who knows enough about the flow of information to answer questions and provide more detail.

The form asks for a legal basis for the processing, we've provided an explanation of what needs to be considered and an example. Within the Healthcare sector, the key basis for processing patient identifiable data is for direct healthcare or healthcare management. Where this is not the case, then the expectation is that pseudonymised or de-identified data will be used.

Most organisations complete an information flow review as part of authorised, if you can review (make sure it accounts for any changes) and provide this it will be a great help. We may need to review the relevant contracts, so you are asked to identify (and potentially provide) these.

You need to identify the type of flow you require, which will enable identification of the legality of the flow. The flow chart on the next page will assist you to identify the type of flow being applied for, which needs to be indicated on your completed form.

C – These forms will be reviewed depending on the type of information requested;

Data Type	Definition	Requested sent to
1	**Personal Data**	**Governance Group**
2	**Sensitive Personal Data**	**Governance Group**
3	**Patient Identifiable Data**	**Governance Group**
4	**Personal Confidential Data**	**Governance Group**
5	**Patient Level Data**	**Direct with Provider Partner to be noted at the Governance Group**

D – Based on the details you provide and the clarification, a recommendation will be made to the NWL Digital ISA Governance Group about whether the information flow can continue or whether only pseudonymised/de-identified data will be provided in future.

E – Approval Process;

Data Management: Change Request Form

- **Data Type 1-4:** If the NWL Digital ISA Governance Group agrees with the decision, they will need to ensure that the business process and analysis of the data is modified appropriately and data templates are updated.

- **Data Type 5:** If the provider partner agreed with the decision, this will be noted at the next Governance Group meeting, the group will then insure that that business process and analysis of the data is modified appropriately and data templates are updated.

If the function does not agree, there is an escalation process where we ask for the rational and potential impact. This is to enable the risk to be assessed and the list of next steps to be prioritised.