

Information Sharing Agreement: Liverpool Vaccination & Immunisation Dataflow

Agreement Commenced: Date of signature
Agreement expires: 01/04/2021
Unique Reference: 0026



Business Intelligence Team

Change History

Version	Date	Author	Details
1.0	19.03.18	LB	Document created
1.1	09.04.18	LB	Changed references to Liverpool Community Health to Merseycare NHS Foundation Trust.
1.2	01.05.18	LB	Added further clarification to specific legal basis for this data flow (see sentence in bold).
1.3	24.05.18	LB	Changed references to HSW and APMT to CHIS system and CHIS team to reflect arrangements made by Merseycare to process the data more effectively.

Summary and Benefits of the Extract

This Information Sharing Agreement (ISA) outlines the specification and information governance arrangements relating to a patient-level data extract which Liverpool CCG would extract and transfer to MerseyCare NHS Foundation Trust **on behalf of General Practice**.

The purpose of this extract would be the upload of General Practice vac & imm data to the CHIS system. CHIS is the system used to store vac & imm details of children in the city and the data source used to identify children who have not had their routine vaccinations, so that they can be targeted by the Active Patient Management Team.

There are known problems with the quality of the data held within the CHIS system, due to its reliance on manual updates upon the receipt of paper forms. To validate the lists of children that require vaccination, the APMT admin support currently have to telephone and / or fax practices resulting in extra work for both the team and general practice, or the nurses themselves have to log in to practice systems to check the immunisation status of the patients (because admin staff have no access to practice systems as part of the iLINKS sharing agreement).

Having a process in place to extract and upload the EMIS general practice data into the CHIS system will ensure that the correct children are targeted for immunisation and mitigate the risk of over-vaccination. In addition it will reduce the burden on practices dealing with telephone calls from the team and the amount of clinician time spent on data reconciliation. It should be noted that this extract will mostly cover data that should have already be shared with MerseyCare NHS Foundation Trust in paper form.

Extract Frequency

This will be a weekly extract

(This is to help avoid the APMT contacting parents to arrange the vaccination of children who have been very recently vaccinated.)

Extract Parameters and uses of the data

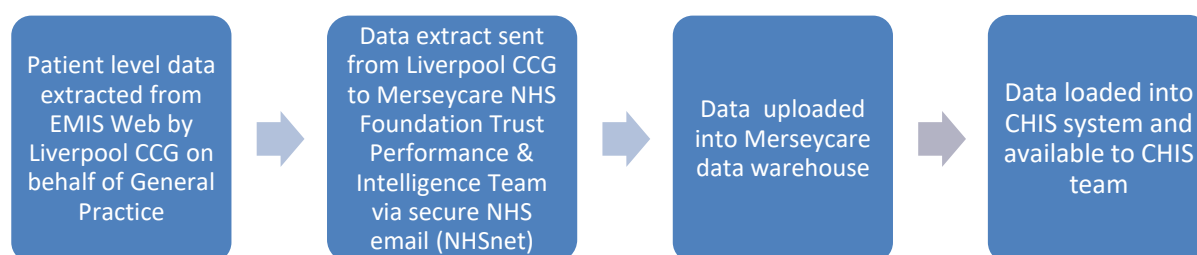
The sole use of the data contained within this extract is for the reconciliation of the childhood vac & imm data held by MerseyCare NHS Foundation Trust with the data held by General Practice. This sharing agreement does not permit any other use of the data.

The extract parameters are below. Search population: Those aged 0-19 with any of the following codes EVER,

Codes	Term	Rules	Date Range
NHS Number			
Date of Birth			
Full Name			
Practice Code			
8I3x	MMR vaccination declined	Most recent	EVER
8IA4	Hib/Men C vaccination declined	Most recent	EVER
68Nh%	Meningitis C immunisation refused	Most recent	EVER
8I3Q	Pneumococcal vaccination declined	Most recent	EVER
8IAX	Diphth, tet, acell pertuss, inact polio imm declined	Most recent	EVER
8IHC%	Meningitis B vaccination declined	Most recent	EVER
8IEM%	Rotavirus vaccination declined	Most recent	EVER
8I2s	Rotavirus vaccination contraindicated	Most recent	EVER
8I23P	Meningitis B vaccination contraindicated	Most recent	EVER
8I2E	Pneumococcal vaccination contraindicated	Most recent	EVER
8I232	DTap/IPV vaccination contraindicated	Most recent	EVER
8I233	DTap/IPV/HIB vaccination contraindicated	Most recent	EVER
8I231	Hib/Men C vaccination contraindicated	Most recent	EVER
68NI-1	MMR vaccine contraindicated	Most recent	EVER
68NQ	Pertussis vaccine contraindicated	Most recent	EVER
65a0	1 st diphth tet acell pertus, haem influ b, inactive polio vac	All Codes	EVER
657L	First pneumococcal conjugated vaccination	All Codes	EVER
65d0	First Rotavirus Vaccination	All Codes	EVER

65710	First Meningitis B Vaccination	All Codes	EVER
65a1	2 nd diphth, tet, acell pertus, haem influ b, inactive polio vacc	All Codes	EVER
65d1	Second rotavirus vaccination	All Codes	EVER
65a2	3 rd diphth tet, acell pertus, haem influ b, inactive polio vacc	All Codes	EVER
657M	Second pneumococcal conjugated vaccination	All Codes	EVER
65711	2 nd Meningitis B vaccination	All Codes	EVER
65b	Haemophilus influenza type B and meningitis C vaccination	All Codes	EVER
65M1	Measles/mumps/rubella vaccin	All Codes	EVER
657N	Third pneumococcal conjugated vaccination	All Codes	EVER
6571A	Booster meningitis B vaccination	All Codes	EVER
65I9	Booster diphth, tetanus, acellular pert, inactive polio vacc	All Codes	EVER
65I8	Low dose diphth, tet, acellular pert and inactive polio vacc	All Codes	EVER
65MC	MMR vaccination – 2 nd dose	All Codes	EVER
653	Tuberculosis (BCG) vaccination	All Codes	EVER
65F1	1 st Hepatitis B vaccination	All Codes	EVER
65F2	2 nd Hepatitis B vaccination	All Codes	EVER
65F3	3 rd Hepatitis B vaccination	All Codes	EVER
65F6	4 th Hepatitis B vaccination	All Codes	EVER
65F7	5 th Hepatitis B vaccination	All Codes	EVER

Extract Process and Data Management



The data extraction from EMIS web will be stored temporarily on the CCG secure network for the purposes of transmission to MerseyCare NHS Foundation Trust. The data will be transmitted to MerseyCare NHS Foundation Trust in the form of CSV files via the CCG Patient Identifiable Data (PID) NHS net account (liverpool.pid@nhs.net). This is an acceptable form of data transmission of patient identifiable data. The information will then be immediately deleted from the CCG network.

Governance and Security

Data Governance

It is essential that all processing and use of personal data is in line with the General Data Protection Regulation (GDPR). In order to protect the rights of individuals there is a statutory duty placed on those who decide 'how' and 'why' such data is processed – the 'Data Controller'. The Data Controller for this General Practice extraction is the GP Practice as they are the statutory body. Therefore all proposed use of the data must be in agreement with GP practices. The CCG will only be acting as a 'Data Processor' for this data ensuring that it is processed for the purposes it is collected and in accordance with the GDPR and other best practice guidance e.g. the UK Government:

- Confidentiality: NHS Code of Practice
- Information Security Management: NHS Code of Practice
- Records Management Code of Practice for Health and Social Care 2016

This essentially means that **ALL** decisions regarding the use of the data rest with the GP Practice. The Data Processors cannot utilise or disclose this information to a third party e.g., Department of Health, without the express permission of the Data Controller, unless covered by the terms of this agreement.

The information will only be used in accordance with the specific purpose that it is provided for and will be at all times treated as confidential and handled in a secure manner.

The shared information will **not** be used for the following:

- Advertising, Marketing & Public Relations
- Trading/sharing in personal information
- Performance and / or contract management

Security of the servers/data warehouse

Data will be warehoused on a secure server hosted by iMerseyside.

- Servers have routine, auditable back up procedure to prevent data loss
- Secure anti-virus software
- Servers in secure room with key access and log book for access
- Building has swipe card access for every floor.
- Computers have time out screens and screen lock functions for users.
- Users have secure password to network that is forced to change every three months.
- This process is regularly audited by external auditors to ensure it is fit for purpose

Legal basis for Information Sharing

The data items shared contain the patient identifiable items of NHS number, date of birth and full name.

The legal basis for the sharing of this data is Direct Patient Care. In legal terms the following Conditions under GDPR are engaged:

Processing Personal Data - Article 6

6(1)(e) Necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller

Processing Sensitive Personal Data – Article 9

9(2)(h) Necessary for the reasons of preventative or occupational medicine, for assessing the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or management of health or social care systems and services on the basis of Union or Member State law or a contract with a health professional

Subject Access

Subject access requests will be dealt with by the data controller in accordance with the provisions of the General Data Protection Regulation.

Complaints

Complaints will be dealt with in accordance with Liverpool CCG Complaints Policy.

Transmission

In line with Department of Health recommendations, the use of laptops or other portable media for storing/transferring person identifiable or other sensitive information is not allowed under this agreement unless it is encrypted to standards approved by the DoH. Data will be transmitted via approved secure routes, in this case NHS net to NHS net email.

Information breaches

Partners will take steps to avoid any breach (intentional or otherwise) or disclosure to third parties outside the remit of this Agreement. Breaches must be reported through Liverpool CCG Incident reporting procedures, fully investigated and a report provided to Liverpool CCG.

Any Serious Untoward Incidents occurring within the scope of the information shared under this agreement must be reported to the participating organisations within 1 day of the incident occurring. The SUI must be fully investigated. The GP practices reserves the right to be informed at every stage of the investigation. Disciplinary action will be the responsibility of the organisation where the incident has occurred. This agreement will be reviewed in light of any lessons learnt from such incidents.

Information will only be accessible to those authorised by this agreement or for whom it is essential to access the information to complete the purpose of the sharing.

Confidentiality

Partner organisations must have confidentiality clause within staff contracts of employment and or require staff participating in this agreement to sign confidentiality agreements. Staff must have current CRB checks where agreements require the sharing of sensitive personal data (GDPR Special Categories of data) in particular children's data. Where training needs to meet the requirements of this agreement are assessed and identified, each organisation will ensure that the resource is made available to staff.

Fair Processing

The Data Controller (in this case the GP Practice) must inform patients how their data is being used, to meet the first GDPR Right to be Informed, through the GP Practice Privacy Notice.

Patient Confidentiality and Opt Out

The NHS Manage Your Choice service is for patients to request that their confidential patient information is not used beyond their own individual care.

If a patient decides to opt out, this will be respected and applied by NHS Digital and Public Health England. These organisations collect, process and release health and adult social care data on a national basis. An opt-out will only apply to the health and care system in England.

As these projects are for direct care, this opt-out does not apply.

However, patients' data will not be shared if any of the read codes listed below are included on their record or if a practice marks their records as 'private' from within the clinical system.

93C1	Refused consent for upload to local shared electronic record
93C3	Refused consent for upload to national shared electronic record
9M1..	Informed dissent for national audit
9R1..	Confidential patient data
9R11	Conf data- patient not to see
9R12	Conf data- not to be reported
9R13	Conf data- staff not to see
9R14	Conf data- paramedics not to see
9R15	Conf data- other Dr not to see
9R1Z	Confidential data NOS
9Nd1	No consent for electronic record sharing
9Nd9	Declined consent for Primary Care Trust to review patient record
9NdH	Declined consent to share patient data with specified third party
9NdJ	Consent withdrawn to share patient data with specified third party
9Oh8	Personal risk assessment declined
9Oh5	Multi-professional risk assessment declined
9Nu4	Dissent from disclosure of personal confidential data by HSCIC
9Nu5	Dissent withdrawn from disclosure of personal confidential data by HSCIC

Dissemination

Copies of this agreement will be provided to each of the signatory organisations. A master copy will be held by Liverpool CCG. Liverpool CCG will support any changes or amendments to this agreement.

This information sharing agreement will be adopted by the signatory organisations. Key staff will be identified in each organisation to ensure that the protocols in this agreement are adhered to.

Information Governance

All signatories to this agreement are required to have approved Information Governance Policies in place that state the legal, ethical and professional obligations to protect service user information. All signatories are also required to have submitted a compliant Information Governance Toolkit in March 2018, and should now be working to submit a compliant Data Security and Protection Toolkit in March 2019, and every year thereafter.

Signatories to this agreement must ensure that all staff, contractors or other third parties who are involved in the processing of information covered by this agreement have received appropriate annual Information Governance training.

This agreement has been subject to a Data Protection Impact Assessment.

Monitoring & Review

Review of this agreement will be overseen by Liverpool CCG, with reference to the signatory organisations, and in particular if there are changes to the agreed purpose or processes. This document will also be reviewed whenever there are changes to legislation or guidelines that may affect the sharing of the information covered by the agreement.

Staff are required to report any adverse incidents to the Business Intelligence Team that may affect the validity of the statements in this agreement and any breaches of security or confidentiality.

Any queries relating to this agreement should be addressed to Liverpool CCG.

Effective Date

This ISA is considered to be effective following signature of all parties and from the date on the signature page of the agreement unless prior authorisation to share has been approved by the Caldicott Guardian.

Information Sharing Agreement

You agree to share the specified extract against the parameters specified within this document.

GP Practice

GP Practice	
Address	
Contact Details	
Signature	
Name	
Designation	
Information processing lead for Practice including contact details	
Deputy Information Processing lead for Practice	

Liverpool CCG

Signature of Caldicott Guardian	
Name	
Contact Details	

Date of expiry: 01.04.2021