Data Protection Impact Assessment

Project / Work Stream Name	**Birmingham & Solihull, Coventry &Warwickshire, Hereford& Worcestershire) Collaborative Shared Care Record**
Project Implementation date	TBC

Version Control

Version	1.1
Status	Final
Date	13/05/2021
Reviewed by	
Author	
Approved Date	03/06/2021

Revision History

0.1	C&W DPIA changed to ICO template
0.2	Reviewed
1.0	Changes made after consultation with C&W IGAG • CCROA definition added • Large scale processing defined • Risk scoring changed to 5x5 matrix • Updated processor DSPT compliance to 20/21 • Minor corrections to grammar and spelling • Added definition of direct care • Added list of legislation
1.1	Section 2.1 Corrections to architecture • **Edge Gateway** - takes structured data from an organisation's system and holds it in a cloud hosted repository specific to that organisation

	• **Operational Data Store:** where an organisation's system does not have an integration engine or API built, data is extracted using batch files and then stored in the Operational Data Store. Created care plan will also be held in this repository (while this functionality exists there is no current plan to utilise it) Added BSOL data set Added appendix E Public Engagement Plan and Report Added updated ISO 27001 certificate for Intersystems Added appendix F Privacy Notice

Submitting controller details

Name of controller	
Subject/title of DPO	
Name of controller contact /DPO (delete as appropriate)	

Step 1: Identify the need for a DPIA

Explain broadly what project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.
Birmingham and Solihull (BSOL) Integrated Care System (ICS), Coventry and Warwickshire ICS, and Herefordshire and Worcestershire ICS are working collaboratively to develop an integrated health and care system (known as the Collaborative Shared Record) that would enable the sharing of health and social care data to facilitate the transformation of health and care services across traditional organisational and technological boundaries. The need for an integrated health and Social care system has been driven nationally in line NHS Long Term Plan for digital transformation. Across the Country, health and care systems are facing an increasing demand for their services, driven by an aging population with more complex needs, a shrinking workforce and advances in medicine and technology that are driving up expectations and the cost of care. A vital component of Birmingham & Solihull, Coventry & Warwickshire, Herefordshire & Worcestershire) Collaborative Shared Care Record programme is the ability to create a joined- up health and care record that spans their population. The Collaborative Shared Record programme aims to provide 'view only' access to identifiable data for purposes of direct care provision and administration by all parties, taking into account the complexity of people's lives and their over-lapping health and social needs. The primary benefits of the sharing, particularly for Direct Care and Administration are anticipated to be: • Better outcomes and more efficient health social care delivery for patients/service users/client irrespective of technological or organisational boundaries. • Better use of resources so that residents receive the right care the first time around thereby reducing referrals, Accident &Emergency (A&E) attendances and inpatient admissions through improved data sharing and early intervention. • Improved availability of data for health and care professionals to enable them to make more informed decisions about the health/care of their patients/users of services' • Avoidance of duplicate investigations improving patients/users of services' experience • Improved safety for patients/users of services' and care professionals due to increased awareness of key patient information e.g. prescribed medications. All of the partner organisations to the Collaborative Shared Care Record will be joint controllers in respect of any personal, or special categories of personal data that they process.

All of the joint controllers will be signatories to the Collaborative Data Sharing Agreement. See appendix A for the full list of joint controllers.

Intersystems are the Processor and shall be required to:

- Demonstrate compliance with the Data Security and Protection Toolkit (DSPT) and/or security management and, quality assurance standards (ISO 27001 and 9001) and provide evidence of Statement of Applicability.
- Enter into a Data Processing Agreement/Contract with the Lead Authority in connection with Call-Off Agreement
- Maintain Records of Processing Activities (RoPA)
- Put in place appropriate technical organisational measures for the protection of personal data that will be processed.
- Complete Cloud Risk Assessment questionnaire for the use of Cloud technology
- Ensure its staff are appropriately vetted
- Ensure that all its staff who would access to personal information (for the purposes of maintenance and support) are compliant with data security and protection training

Step 2: Describe the processing

2.1 Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

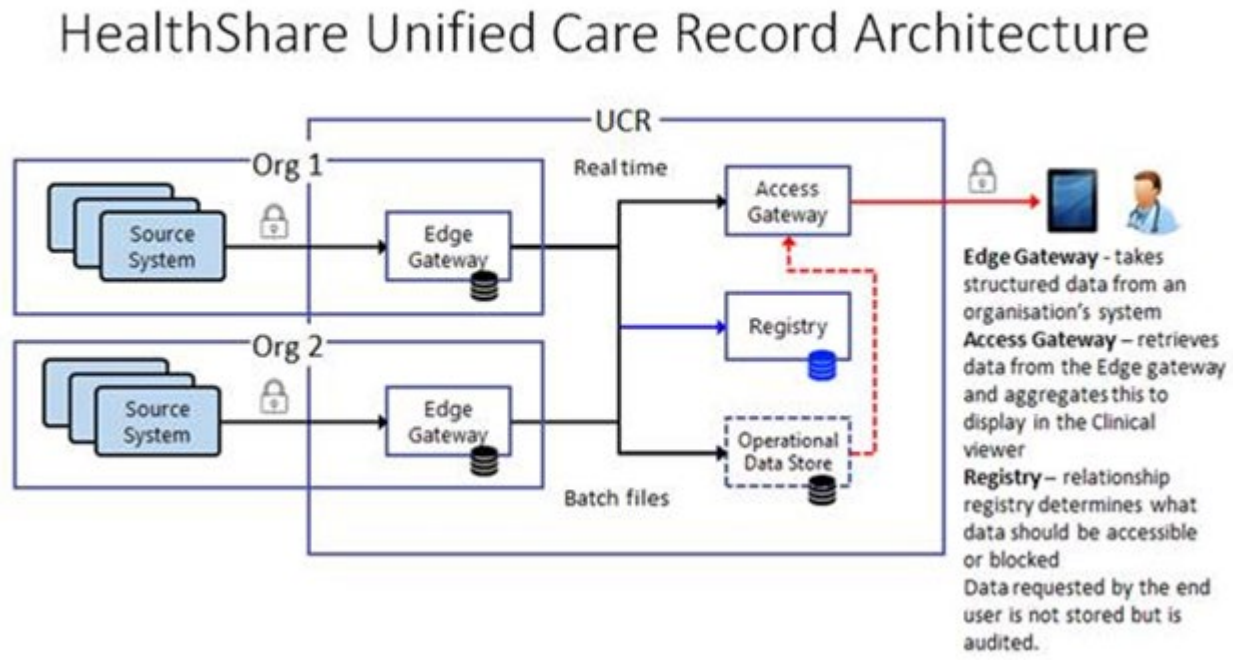
2.1.1 Describe the nature of the processing

To develop the Collaborative Shared Care Record, the partners have procured the services of “Intersystems” (software/system supplier, Cloud Hosting and Processor). to The Intersystems solution will connect electronic systems of local health and social care providers via a central system (‘Information Exchange’) .The system will provide their registered health and social care professionals (“Registered Professionals”), supported by any Non-registered Support Staff, with access to read only views of limited datasets, consisting of health and social care data held by the respective Parties (“Shared Personal Data”), with the view to:

- Developing integrated health & social care
- Ensuring efficiencies of scale by reducing time to locate a full history of care provided in other settings
- Improving quality of care by creating fully visible care records
- Saving patients/users of services' lives by allowing imminent access to crucial information in emergency situations

Data is processed for the purpose of providing direct care and administration. The term 'direct care' shall mean all clinical, social or public health activity which contributes directly to the prevention, investigation and treatment of illness or the alleviation of suffering of individuals and shall include the assurance of safe and high quality care and treatment through local audit (identified patient safety), the management of untoward or adverse incidents. The term 'users of services' shall describe those individuals who receive or are eligible to receive social care services without seeking to impose any other meaning or interpretations upon it or them

For clarity and completeness Intersystems term "Health Share" is synonymous to Information Exchange (IE)



The HealthShare environment will be accessed by an authorised health and/or social care professional via their respective source health or social system (e.g. EMIS, Adastra, Mosaic etc). Depending on the source system, there will be capability to request view access for: -

- **Edge Gateway** - takes structured data from an organisation's system and holds it in a cloud hosted repository specific to that organisation
- **Access Gateway** – retrieves data from the Edge gateway and aggregates/matches the data to display in the Clinical viewer
- **Registry –** relationship registry determines what data should be accessible or blocked. Data requested by the end user is audited.
- **Operational Data Store:** where an organisation's system does not have an integration engine or API built, data is extracted using batch files and then stored in the Operational Data Store. Created care plan will also be held in this repository (while this functionality exists there is no current plan to utilise it)

2.1.2 Will this new system, process or data flow include data which was not previously collected?

No. The system allows data that is already collected in participating organisation's systems to be viewed in one place.

2.1.3 Does the project involve linkage of personal data with data in other collections, or significant change in data linkages?

Yes. The Collaborative Shared Care Record connects information held in multiple electronic health and care systems from partner organisations about the same person, to provide a much wider record.

This will provide health and/or social care professionals with the data they need to make more informed clinical and care decisions.

2.1.4 Will the data be shared on with any other organisations?

The shared data will not be shared with any other organisations outside the scope of the DSA

Personal and special categories of personal data shared for the purpose of Direct Care shall be:

- Adequate - sufficient to properly fulfil your stated purpose
- Relevant - has a rational link to that purpose and,

Limited (not excessive) to what is necessary for the purpose for which they are shared /processed.

InterSystems have confirmed that no sub processors are involved in the processing of personal data

2.1.5 Where will data be held?

Personal, special categories of personal data shall flow from the partner's source system, and shared data will be held primarily on each Controller's health or care system (e.g. EMIS, Adastra, Liquid Logic).

Most of the health or care partners shall use their integration engines or Application Programme Interface (API) to flow read only view data via the "Information Exchange" into Intersystems' HealthShare Instance environment to create a shared care record.

Where a partner organisation does not have an integration engine or API, data will be extracted using batch files (automated extracts) and then stored on Intersystems' Operational Data Store within the HealthShare environment.

Data will be held in the private InterSystems cloud environment hosted entirely in the UK

2.1.6 What format will data be stored in?

Data will be stored in Health Share via XMLformat within the cache databases on each Edge Gateway, this is wholly owned by InterSystems Limited.

2.1.7 What security measures are in place to protect the information?

Physical security is provided InterSystems Limited, accredited to ISO27001, which covers services provided in the UK by InterSystems Limited.

Information security is supported through password controls, role-based access controls and protected through active directory authorisation and each organisation's local policy on usage of data. InterSystems Limited advises that its security model can be tailored to meet the requirements which are placed on it by local organisations, and it is these will be considered by the Clinical Design Authority and implemented accordingly.

The Processor – Intersystems shall use 'user access authentication' mechanisms to ensure that all instances of access to any Personal Data in the system are auditable against an individual. The system can collate an audit trail of every user who has accessed shared personal data and record the following:

- name of staff member accessing the system
- usage detailing date/time of log-in, log-out including auto-logout;
- views broken down by data subject's NHS number/general demographics;

- searches/requests for shared personal data by data subject's NHS number/general demographics;
- touchpoints and usage report

The following functionalities are also available within the HealthShare environment:

- The system can track and audit all user access, including who, when, where and what was accessed and system administration functions such as application and interface configuration.
- The system can generate audit reports at when needed by authorised users to interrogate the audit logs using search criteria such as date, user ID, data subject ID, function, application etc.
- The audit database is capable of achieving data retention objectives like archive or copied to another storage system, then truncated.
- The system track and audit all user searches (to help track phishing for example) including the search criteria used and the results received. The audit trail can show what data was available to the user at the time of the request.

Access controls will be used to limit or prevent access to certain classes of information.

Databases are held on an encrypted storage device with 256-bit AES encryption (at rest). All data in transit is encrypted using TLS.

2.1.8 How will authorised staff access and amend data?

Role-based access controls will apply, and access will be linked to the active directory (or smartcard access) in each organisation; these access controls have been approved by the clinical design authority in each ICS..

User "access level" shall be minimised and managed in line with the Role Based Access Control (RBAC) within the source system. RBAC within the system shall be granted on strictly on need-to-know basis and, will be determined by each user's job role and the level of access they have within their source/native system which is based on locally developed "Local Role Profiles". Therefore, it will be the responsibility of each organisation to determine the level/hierarchy of access by each user would have.

Access shall be granted strictly on "need to know basis" in accordance with the 3rd data protection principle and 4th Caldicott Principle

The system provides is a 'read only view data' from source of systems. It does not provide facilities to edit/add or change the content of a record that originates from another system. Updates, amendments and overlays depend on changes being recorded on the originating system.

Access to the system shall use Cache' delegated 'user access authentication' mechanism which performs the authentication and determines roles, and there are several types of authentication possible within the system, for example, through Smartcard controls that each user has within their source system, and two factor authentication dependents on the technical set up at each organisation.

There are two main types of job roles within the Integrated health and care system [administrative (back end)] and [application (front end)] which can be split into multiple layers of RBAC matrix. The two main job roles are:

- **Application** level roles – e.g. Clinicians, Social Workers, Admin-Clerical Staff, etc.
- **Database** level roles – e.g. "Database Administrator", "Interface Developer, security configuration etc (system maintenance purposes).

Data can only be amended in the controllers source systems and not in the Integrated Care Record

2.1.9 What business continuity plans are in place in the case of data loss / damage as a result of human error / computer virus / network failure / theft / fire / flood / other disaster?

The Information Exchange supplier - Intersystems has produced an Information Security Management document would localise this to the Collaborative Shared Care record needs This also contains reference to the BCP below.

Intersystems' BCP has embedded above defines how Intersystems invoke it BCP and disaster recovery.

2.1.10 Is there a useable audit system in place for the asset?

Yes; All system events are audited and the audit records are held in a read-only database which is used for audit reporting. Both read and write events are audited showing the event type, date and user - the full data record that was returned to the user at that time is also included.

The system is auditable with access by each contributing organisation. Local authentication and security models are leveraged and used. The Intersystems' audit tool screen captures the landing page of the record being visited by the user which contains personal data of individuals.

The Processor – Intersystems shall use 'user access authentication' mechanisms to ensure that all instances of access to any Personal Data in the system are auditable against an individual. The system can collate an audit trail of every user who has accessed shared personal data and record the following:

- name of staff member accessing the system
- usage detailing date/time of log-in, log-out including auto-logout;
- views broken down by data subject's NHS number/general demographics;

- searches/requests for shared personal data by data subject's NHS number/general demographics;
- touchpoints and usage report

In addition, each Partner will be required to audit access to the HealthShare environment and report any anomalies to the collaborative central team, who will in turn inform other parties and Intersystems.

Data controllers audit scope and requirements are to be approved by the Collaborative Care Record Oversight Authority (CCROA).

The Collaborative central team will work closely with the system supplier and processor to facilitate the audit of unusual activity and will audit requests from organisations where there is suspicion of unauthorised access – This will / can include a screenshot of what the user could see at the time they accessed the records (appendix C)

2.1.11 What training have users of the other organisations had in confidentiality of personal data?

Each partner organisation is responsible for ensuring that their staff (agency, permanent and temp staff) with access to Information Exchange are compliant with their mandatory data security training.

2.2 Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

2.2.1 Who will be involved in the processing activity

Partner organisations - See appendix A and Appendix B

Each partner organisation will be responsible for their own ROPA

The processing will involve all patients/service users in the ICS's:

- Birmingham and Solihull
- Coventry and Warwickshire
- Herefordshire and Worcestershire

The potential volume of data subjects is dependent on the number of patients/service users having health or social care at the partner organisations. There will be processing of data subjects on large scale

[1]Birmingham and Solihull ≈1.4m

Coventry and Warwickshire ≈1m

Herefordshire and Worcestershire ≈0.8m

Total ≈3.2m

Staff data will also be processed for the partner organisations

2.2.2 What data will be processed

The approved data fields are:

Birmingham and Solihull

CCROA Data Set by Organisation.xlsx

Coventry and Warwickshire

Overview of CWICR Datasets v2 1204202

Herefordshire and Worcestershire

Shared Record Dataset .docx

2.2.3 Records retention

Records will be retained in the partners host systems in line with the relevant health and social care Records Management Code of Practices.

For data held within the Information Exchange, CCROAG will approve system wide automatic retention periods which take into account the statutory retention periods.

[1] Patients Registered at a GP Practice January 2021 - NHS Digital

2.3 Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

2.3.1 What is the nature of your relationship with the individuals?

Patients or service users of the partner organisations. Each Partner to the Collaborative Shared Record provides either health or social care service to the individuals - patients/service users for the purpose of direct care. The individuals are therefore registered as either a patient/service users with each of Birmingham and Solihull (BSOL) Integrated Care System (ICS), Coventry and Warwickshire ICS, and Herefordshire and Worcestershire ICS health or care partner.

2.3.2 Do they include children or other vulnerable groups?

Yes.

2.3.3 Would they expect you to use their data in this way?

Public consultation undertaken by the three ICS's has shown that people expect health and social care organisations to share information for direct care purposes.

Patients/service users may not expect certain categories of health data to be shared with social care staff. This has been considered and certain fields will be restricted to health care staff only (see appendix D).

2.3.4 How much control will they have?

Each Data Subject will have the right to:

- To access, view or request copies of their personal information by contacting their relevant health/social care provider
- Request rectification of any inaccuracy in their personal information by contacting their relevant health/social care provider
- Raise an objection to having their health and social care record integrated by contacting their relevant health/ social care provider or the central team (details in appendix C)
- Contact their relevant health/ social care provider to restrict the processing of their personal information where:
    - accuracy of the data is contested.
    - the processing is unlawful or,
    - where their data is no longer needed for the purposes of the processing.

2.3.5 Is it novel in any way?

No, ICR's are in place across the country.

2.4 Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

The intended outcomes are to enable health and social care access to information about an individual's health and social care needs, ensuring the best joined up care can be delivered for those who need it, by allowing the delivery of care and support at the right time in the right place, reducing disruption to individuals by linking up data systems, this will create fewer gaps in relation to referrals from one healthcare/social care provider to another for treatment/care and social care provisions.

2.4.1 Who will use the new processing activity and have access to the data?

Access will only be granted to health and social care professionals who are involved in an individual's care and technical staff providing support for the ICR. Access to Shared Personal Data will be restricted to 'view only' access with an 'extended view' for registered (healthcare) professionals and a 'restricted view' for registered social care professionals.

It will be a condition that all Parties' staff with access to the shared personal data will have a legitimate relationship with the data subject in question.

Registered Professionals will require a Legitimate Relationship with the user of services which will be present if any or all of the following criteria are met:

- The individual presents themselves to the Registered Professional to receive (health or social) care.
- The individual agrees to a referral from one Registered Professional to another.
- The individual presents to a registered professional in an emergency situation.
- The relationship if underpinned by a legal duty to share (e.g. safeguarding for a child or vulnerable adult).

Non-registered (administrative/secretarial) Support Staff will have a right of access if any or all of the following criteria are met:

- The individual presents themselves to those staff for the purposes of care e.g. NHS 111.
- The Staff member is professionally supervised by a Registered (health or social care) Professional with a Legitimate Relationship to the individual.
- The Staff member is managerially directly responsible to a Registered Professional with a Legitimate Relationship to the individual for the lawful use of confidential information.
- The citizen has given explicit consent that the member of Staff should access all or part of their confidential information.
- The Staff member is registered on a voluntary register approved by the Professional Standards Authority and has a Legitimate Relationship to the individual.

Access by IT staff will be controlled via robust data processor agreements. Each Party might have their own processors (sub-contractors) to facilitate the interface between the HIE and their own health/social care system(s). Additionally, there might be one jointly appointed processor for the ongoing support and maintenance of the SCR. The minimum requirements (technical/organisational measures and security standards) for all DPAs (including the jointly appointed processor for the SCR) will be stipulated in the DSA (Schedule 3).

Step 3: Consultation process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

3.1 Public consultation

The public has been extensively consulted on the proposed Collaborative Share record. Feedback has been gathered and taken into account in the planning stages for the project.

3.2 Stakeholder consultation

Extensive stakeholder engagement has taken place including technical staff, IG professionals, legal advisors, communications teams and senior leadership.

The DPIA will be jointly reviewed by each ICS's local information governance group.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

4.1 what is your lawful basis for processing?

The lawful basis for processing information is based on the following legislation:

UK GDPR / DPA 2018

Under UK GDPR there must be a valid lawful basis to process personal data. For UK GDPR sharing information for the Collaborative Share record is on the basis of Public Task where "processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller".

Article 6(1) of the GDPR is the condition for lawfully processing data for delivering direct care as part of the Collaborative Share record:

6(1) for the performance of a task carried out in the public interest or in the exercise of official authority…'

Article 9(2)(h) of the GDPR is the condition for processing 'data concerning health' (personal data relating to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status) for direct care as part of the Collaborative Share record:

9(2)(h) medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems…'

Additional lawful basis that receiving parties may rely on in specific circumstances:

Emergency situations where the data subject is incapable of giving consent

- Art 6(1)d ('vital interests')
- Art 9(2)c ('vital interests')

Safeguarding of vulnerable adults and children

- Art 6(1) c ('legal obligation to which the controller is subject')
- Art 9(2) g GDPR ('where the processing is necessary for the purposes of substantial public interest (protection of vulnerable individuals')

Staff Data Processing

Access control and audit logs of user credentials used for authentication purposes

- Art 6(1)b GDPR ('processing is necessary for the performance of a contract to which the data subject is party)

4.2 Additional requirements for data processing

DPA 2018 Schedule 1, Part 1 (2) (1 & 2) Processing is necessary for health or social care purposes for the purposes of:

(h) Preventive…medicine, medical diagnosis

(d) the provision of health care or treatment the provision of social care or

(h) the management of health care systems or services or social care systems or services

The requirement to inform the patient and document access to the patient record using the normal controls in the provider organisation will remain and be available for audit purposes.

For unscheduled care, the treating clinician will still ask for permission to view the shared record where possible. For scheduled care, on referral, the patient has given permission through implied consent to share relevant information, as outlined in the GMC guidance on confidentiality. Patients still have the right to object to processing.

Section 10 (1)(c) and any relevant condition in Schedule 1 of Part 1 of the DPA 2018:

'Health or social care purposes' means the purposes of:

- preventive or occupational medicine;
- medical diagnosis;
- the provision of health care or treatment;
- the provision of social care, or

• the management of health care systems or services or social care systems or services.

Section 11 of the DPA2018 (1)For the purposes of Article 9(2)(h) of the GDPR (processing for health or social care purposes etc), the circumstances in which the processing of personal data is carried out subject to the conditions and safeguards referred to in Article 9(3) of the GDPR (obligation of secrecy) include circumstances in which it is carried out—

(a)by or under the responsibility of a health professional or a social work professional, or

(b)by another person who in the circumstances owes a duty of confidentiality under an enactment or rule of law.

All partners are subject to a number of legal obligations to ensure that the processing of personal information remains lawful. This includes, but is not limited to the following legislation, standard, statutory and non-statutory guidance.

- UK General Data Protection Regulation (UKGDPR)
- UK Data Protection Act (DPA) 2018
- Common Law Duty of Confidentiality
- Freedom of Information Act 2000
- Human Rights Act 1998 (Article 8)
- Mental Health Act 1983
- Mental Health Act 2007
- Mental Capacity Act 2005
- Health and Social Care Act 2012
- Health & Social Care (Quality and Safety) Act 2015
- Care Act 2014
- Health and Social Care (National Data Guardian) Act 2018
- Public Health (Control of Disease) Act 1984

4.3 How will you prevent function creep?

All parties will be signatories to a DSA that sets out the permitted purposes of the shared data. Any purpose changed must be approved by CCROA and the joint controllers.

4.4 How will you ensure data quality and data minimisation?

Data quality will be the responsibility of the organisation that records the information in their host system. All partners have policies and processes in place around data quality. If incorrect data is found then the data subjects have the right for that data to be rectified.

Data minimisation and necessity will be ensured as the data sets have been approved by the clinical practitioners reference group and data sets only include necessary fields for direct care. In addition, Caldicott Guardian sign-off will be required or equivalent as per partner organisation's governance structure.

Restricted data sets will be excluded from the shared data.

4.5 How will you help to support data subject rights?

4.5.1 Right to be informed

Each partner organisation will publish a privacy notice on its website. A jointly approved template privacy notice will be developed and adopted by the joint controllers.

4.5.2 Right of access

The Data Subject will need to submit a Data Subject Access request, either verbally or in writing to the relevant partner organisation. The partner organisation will be responsible for providing data held within its own linked Health/Social care system. This excludes information that is accessible via the ICR as read only. This will be included in the ICR privacy notice.

4.5.3 Right to rectification

The Data Subject will contact the relevant partner organisation to exercise this right.

4.5.4 Right to erasure

The right to erasure does not apply if the processing is necessary for the purposes of preventative or occupational medicine; for the working capacity of an employee; for medical diagnosis; for the provision of health or social care; or for the management of health or social care systems or services. This only applies where the data is being processed by or under the responsibility of a professional subject to a legal obligation of professional secrecy (eg a health professional).

4.5.5 Right to restrict processing

See right to object

4.5.6 Right to data portability

The Data Subject will contact the relevant partner organisation to exercise this right.

4.5.7 Right to object

The right to object will be managed centrally and a process is in place to apply the objection to all controllers. This will require continued processing of limited demographic data in order to apply the objection.

The controller may put in additional measures to stop the flow of data at their boundary'. This will be locally decided.

4.5.8 Rights in relation to automated decision making

The ICR uses automatic matching of patients across the partner organisations using demographic details. This is not considered automated processing as defined by the ICO as it does not have a legal or similarly significant effect on the individual. A legal effect is something that adversely affects someone's legal rights. Similarly significant effects are more difficult to define but would include, for example, automatic refusal of an online credit application, and e-recruiting practices without human intervention.

The ICR data is not used for automated profiling of individuals.

There is a manual process in place for correcting mismatched or unmatched patients.

4.5.9 Does the National Data Opt-Out apply to this process? If yes how will it be implemented?

The NDOO does not apply to processing for direct care purposes.

If secondary uses for the ICR are approved by the governing body in the future this may need to take into account the NDOO and processes will need to be established to ensure it is applied constantly and effectively. This will include a variation to the DSA and Privacy Notice.

4.5.10 What measures do you take to ensure processors comply?

A data processing agreement will be in place for the data processor which includes all the necessary clauses under UK GDPR

4.5.11 How do you safeguard any international transfers?

N/A. All data is processed fully within the UK

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Data availability if the ICR becomes unavailable. Intersystems provide a resilient system across two data centres so this scenario only occurs where the ICR is unavailable if both instances fail controllers will revert to source systems; use other means of ascertaining clinical and social care histories etc	2	2	4
Loss of data feeds with missing information from one or more partners. ICR will display a system status message, advising to use other means of ascertaining clinical and social care histories etc.	2	2	4
Inappropriate data trawling or staff accessing data without a legitimate relationship to the patient Access to the ICR is restricted to only those agreed representatives of each party to the DSA. Each party offers assurance of completed DP training by all with access (by signing up to the DSA). Audit reports on usage and unusual data patterns; widened disciplinary processes will apply to inappropriate ICR usage	3	4	12
Inaccurate information given to the public via out of date or different privacy notices amongst joint controllers	3	3	9
Data breach or cyber security incident affecting the HIE	2	5	10

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5				
Risk	**Options to reduce or eliminate risk**	**Effect on risk**	**Residual risk**	**Measure approved**
Inappropriate data trawling or staff accessing data without a legitimate relationship to the patient	Audit schedule to be agreed by CCROA	Reduced likelihood to 2	8	Yes included within DSA
Inaccurate information given to the public via out of date or different privacy notices amongst joint controllers	Standard privacy notice to be drafted collaboratively and adopted by the organisations	Reduced likelihood to 2	6	Yes included within DSA
Data breach or cyber security incident affecting the HIE	Data breaches affecting the HIE will be managed centrally by CCROA. CCROA will co-ordinate the response and recovery with the partner organisations	Reduced impact to 4	8	Yes included within DSA

Step 7: Sign off and record outcomes

IGAG Advice: IGAG has reviewed the DPIA and are satisfied that the contents meet the requirements of the data protection legislation and provide protection to the rights and freedoms of the data subjects.		
Summary of DPO advice: The DPIA has been collaboratively reviewed between the three Integrated Care Systems and Coventry and Warwickshire Information Governance Advisory Group. This has been approved by this collaboration of IG professionals. I have no objection to this processing activity as the Trust has sufficient lawful basis for the processing and the rights and freedoms of the data subjects have been protected.		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
This DPIA will kept under review by:	C&W Information Governance Advisory Group	The DPO should also review ongoing compliance with DPIA
Approved by	Signature	Date

8. Appendices

Appendix A – Joint Controller Details

Included in schedule 6 of the Data Sharing Agreement

Appendix B – Processor Details

InterSystems Ltd.
Tangier Lane
Eton
Windsor
Berkshire
SL4 6BB

ICO Registration - Z5992070
DSPT submission - 20/21 Standards Exceeded, published on 29/03/2021

Does the organisation have any additional certification?
Yes, documentation provided for ISO2000-1, ISO22301, ISO27001

Appendix C – CCROA Support SOP

Appendix D – Health and Social Care Restrictions

Schedule 1 - Collab DSA.doc

Appendix E – Public Consultation

An eight week engagement communication and engagement campaign was carried out by the programme team in autumn 2020. This included a social media campaign targeted at hard to reach groups and contact with community and faith groups.
The full report on the engagement is attached:

CWICR Engagement campaign report_Wel

Appendix F – Privacy Notice

The collaborative Privacy has been approved and is publicly available at:
https://www.happyhealthylives.uk/our-priorities/digital-transformation/integrated-care-record/privacy-notice/

A statement for all partner organisations to include on their privacy notice has been sent to all partners.

Privacy notice statement for ICR - F