

DATA PROTECTION IMPACT ASSESSMENT TEMPLATE

A Data Protection Impact Assessment (DPIA) is a process that helps an organisation identify and minimise the data protection risks of a project.

This DPIA template must be completed wherever there is a change to an existing process or service, or a new process or information asset is introduced that is likely to involve a new use or significantly changes the way in which personal data is handled or processed.

Project / Work Stream Name	Integrated Care and Wellbeing Record (ICWR) - Herefordshire and Worcestershire Sustainability Partnership (STP)	
Project / Work Stream Leads	Name(s)	John Uttley
	Job title	Programme Director - Hereford and Worcester Integrated Care and Wellbeing Record
	Telephone	07872 417160
	Email	johnuttley@nhs.net
Project Implementation date	The ICWR project is expected to be implemented by 31 March 2021	

Please complete screening questions below which are aimed to highlight problems that need to be addressed, prevent problems arising at a later stage which might impede the progress or success of the project.

Step 1: Complete the Screening Questions			
Q 1	Category	Screening question	Yes/No
1.1	Technology	Does the process introduce new or additional technologies or making changes to existing technologies?	Yes
1.2	Technology	Does the process introduce new or additional information technologies that can substantially reveal an individual's identity and has the potential to affect that person's privacy? <i>E.g. the use of biometric or facial recognition</i>	No
1.3	Technology	Does the process involve a systematic monitoring of a publicly accessible area on a large scale?	No
1.4	Identity	Does the processing involve the tracking of individuals' online or office behaviour or location, or will it be used to offer online services directly to them?	No
1.5	Identity	Does the process involve automated individual decision-making, including profiling to help make decisions significantly affecting the data subject?	No
1.6	Identity	Does the process involve a systematic and extensive evaluation of personal aspects relating to an individual which	No

		is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the individual or similarly significantly affect the individual?	
1.7	Multiple organisations	Does the process involve sharing of personal data with multiple organisations?	Yes
Q2	Category	Screening question	
1.8	Data	Does the process necessitate the use/processing/collection/sharing of any personal data, special categories of personal data or pseudonymised data?	Yes
1.9	Data	Does the process involve new process or significantly change the way in which personal data or special categories of personal data is handled?	No
1.10	Data	Does the process involve processing on a large scale of personal data or special categories of personal data concerning health (including racial or ethnic origin data)?	Yes
1.10.1	Data	Does the process involve the processing of other special categories of personal data such as: genetic data, biometric data, criminal conviction data, sex life or sexual orientation data, philosophical beliefs, or trade union membership?	No
1.11	Data	Does the process involve data matching, consolidating, combining, comparing, cross referencing, or inter-linking of personal data or special categories of personal data from multiple sources?	Yes
1.12	Data	Will the personal data or special categories of personal data be processed out of the U.K?	No
1.13	Exemptions and Exceptions	Does the process relate to data processing which is in any way exempt from legislative privacy protections?	No
1.14	Exemptions and Exceptions	Does the process justification include significant contributions to public security and measures?	No
1.15	Exemptions and Exceptions	Does the project involve systematic disclosure of personal data or special categories of personal data to, or access by, third parties that are not subject to comparable privacy regulation?	No

Answering “Yes” to any of the screening questions above represents a potential data protection risk factor. Please proceed and complete the next section.

Step 2: Overview – Identify the need for a DPIA		
2.1	Is this a new or changed use of personal data or special categories of personal data that is already processed/shared?	New/Changed?
		New
2.2	What is the process/project under consideration?	
	<i>Explain broadly what project/process/work stream 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.</i>	

A fundamental element of the NHS Long Term Plan is the ability to deliver an Integrated health and care system that would enable health and care professionals share information, to enable them make best informed decisions about individuals receiving health and/or care support.

Integrated health and care system (digital transformation) brings together local health and care organisations to transform the healthcare and wellbeing of their population, creating shared leadership and action. To achieve this, Herefordshire and Worcestershire (H&W) Sustainability Transformation Partnership (STP) are working collaboratively to develop an Integrated Care and Wellbeing Record (ICWR) that would enable the sharing of health data and social care data to facilitate the transformation of health and care services across traditional organisational and technological boundaries.

Integrated Care and Wellbeing Record (ICWR) is an integrated electronic health and care record linkage that integrates data from multiple electronic health and care systems in H&W to provide read-only view of a patient's health and/or social care record via the secure Health and Social Care Network (HSCN). ICWR would enable health and care professionals who are directly involved in a patient's care to access the information needed to provide that patient with the best possible care.

How ICWR would work in H&W STP:

1. To develop ICWR, H&W STP has procured the services of "Intersystems" (software and system supplier) who has developed a similar "Interoperability Instance" called "HealthShare" for the Birmingham and Solihull (BSOL) Sustainability Transformation Partnership (STP) and, Coventry and Warwickshire STP to enable them to deliver their integrated health and care record programmes. HealthShare" is currently hosted by University Hospitals Birmingham (UHB) NHS Foundation Trust (FT).
2. As Intersystems' HealthShare Instance has the capability to serve multiple STPs, it was agreed by the H&W STP Digital Board that there was the need for H&W STP to host its ICWR on the same HealthShare Instance as BSOL STP and W&C STP. The benefit realisation include but not limited to:
 - Reduction in cost of duplicating functionalities
 - Cost savings on IT maintenance support, connections, installation, and licenses
 - To Create a level playing field for the future Local Health and Care Record Exemplars (LHCRE) Programme – Pan STP integrated health and care record.
3. Most of the H&W health or care partners shall use their integration engines or Application Programme Interface (API) to flow read only view data into the HealthShare Instance environment to create an ICWR for the H&W Partners. 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. A diagram of data flows is embedded below:

For the avoidance doubt, this DPIA specifically covers H&W ICWR to enable the H&W health and care partners to share information between themselves for the purpose of Direct Care. The DPIA although refers to LHCRE, it does not cover the future LHCRE – Pan STP Programme. Intersystems' HealthShare will be used to create H&W STP's integrated electronic health and care record linkage - ICWR.

<p>2.3</p>	<p>Describe the consultation/checks that have been carried out regarding this project/process of similar nature, whether conducted within your organisation or by other organisations (seeing what else is out there).</p> <p><i>Please provide any supporting information/documents/case studies on projects/process that are similar in nature, and lessons learnt from those projects to mitigate risks.</i></p> <p>For the purpose of this DPIA, the consultation and checks carried out in respect of project/process of similar nature will refer to the ongoing shared record programme in Birmingham and Solihull (BSOL) Sustainability Transformation Partnership (STP), as follows:</p> <p>BSOL STP have been working collaboratively on a similar digital shared record/interoperability solution called Health Information Exchange (HIE), which is due to go-live in January 2021. As explained above “Intersystems” (software and system supplier) who has developed an “Interoperability Instance” called “HealthShare” (currently hosted by UHB NHS FT), enabling BSOL STP to develop its integrated electronic health and care record linkage – HIE.</p> <p>Consultation and Checks</p> <p>As BSOL STP’s HIE and H&W STP’s ICWR will be delivered on Intersystems’ HealthShare platform, and BSOL STP is ahead in delivering its shared record programme objectives, consultation and checks with BSOL STP has enabled H&W STP to learn from the categories of issues that were identified and mitigated during the development of HIE design features. These include:</p> <ul style="list-style-type: none"> • the process for managing access controls within the system. • Patients/service users’ opt-out process • Exclusion of data with sensitive codes (e.g. sexual health/orientation or gender identity disorder) from data flows. <p>For the avoidance of doubt, the above issues have been addressed as covered in this DPIA.</p>
<p>2.4</p>	<p>How does the life cycle of data and processes work?</p> <p>Present and describe how the product generally works (from the data collection, retention to destruction, the different processing stages, storage, etc.), using for example a diagram of data flows (add it as an attachment) and a detailed description of the processes carried out.</p> <p>To develop ICWR, H&W STP has procured the services of “Intersystems” (software and system supplier) who has developed a similar “Interoperability Instance” called “HealthShare” for the Birmingham and Solihull (BSOL) Sustainability Transformation Partnership (STP) and, Coventry and Warwickshire STP to enable them to deliver their integrated health and care record programmes. HealthShare” is currently hosted by University Hospitals Birmingham (UHB) NHS Foundation Trust (FT).</p> <p>As Intersystems’ HealthShare Instance has the capability to serve multiple STPs, it was agreed by the H&W STP Digital Board that there was the need for H&W STP to host its ICWR on the same HealthShare Instance as BSOL STP and W&C STP.</p> <p>Most of the H&W health or care partners shall use their integration engines or Application Programme Interface (API) to flow real-time and read only view data into the HealthShare Instance environment to create an ICWR for the H&W Partners. 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. Created care plan will also be held in this repository.</p>

Diagrams that explain the data flows from participating organisations, their source systems, integration engines, Intersystems HealthShare Architecture, and data retention schedules are embedded below:



ICWR Data
Flow_V5.pdf



H&W ICWR Full
Datasets_V3.docx

Step 3: Describe the nature, scope, context, and purpose of the processing

3.1 How will the data be collected?

Most of the H&W health or care partners shall use their integration engines or Application Programme Interface (API) to flow real-time and read only view data into the HealthShare Instance environment to create an ICWR for the H&W Partners. 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.

The ICWR will be accessed by an authorised health and/or social care professional via their respective source health or social system (e.g. EMIS, Adastral, Mosaic etc). Depending on the source system, there will be a 'button' showing access to the ICWR. Once this button is pressed, a request is being processed in the following way:

- **Edge Gateway** - takes structured data from an organisation's system
- **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.

A diagram of data collection and flows is embedded below:



ICWR Data
Flow_V5.pdf

Care Plans:

Part of the functions in ICWR is to enable health/care professionals to work with their patients/service users to create plans within the system which will be stored in the Operational Health Datastore. The solution is to have just one Care Plan for each patient/service user, which encompasses all the data required by the various clinical pathways that the patient/service user is on.

If a health/care professional creates a Care Plan for a patient/service user and populates the plan (either from data they have entered in their own systems or by starting a care plan in ICWR) then if a health/care professional, in another organisation begins another Care Plan for a different care pathway, they will see

	<p>that there is already an existing Care Plan in place for that patient/service user, that the core information is already populated and so they only have to add the data that is specific to their pathway's Care Plan.</p> <p>Each health/care professional is responsible for the accuracy of the data that they input (including changes), therefore the organisation who employs the health/care professional for the care that they are recording will be the Controller.</p>
<p>3.2</p>	<p>How will data be used? <i>(For example, Direct Care and Administration, public health, evaluation or analytical purposes)</i></p> <p>Personal, and/or special categories of personal data that is processed/shared/viewed by the H&W health and social care partners to the ICWR is for the purpose of Direct Care and Administration, to enable health and/or social care professionals who are directly involved in a patient/service user/client's (an individual) health or social care to access the information needed to provide that individual with the best possible health/care service.</p> <p>The primary benefits of the sharing, particularly for Direct Care and Administration are anticipated to be:</p> <ul style="list-style-type: none"> • Better outcomes and more efficient health social care delivery for patients/service users/client across Herefordshire and Worcestershire 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 • Avoidance of duplicate investigations improving patient experience • Improved safety for patients and care professionals due to increased awareness of key patient information e.g. prescribed medications.
<p>3.3</p>	<p>How will the data be stored? <i>Examples of Storage include bespoke system (eg EPR, Emis & other clinical systems, SharePoint, data repository, Network Drives, Filing cabinet (office and location), storage area/filing room (and location) etc</i></p> <p>Except for Care Plans which will be newly created record, most of data flows into the HealthShare system will remain stored in each Controller's source system and cannot be edited or restored by the data recipient partner. Most of the H&W health or care partner shall use their integration engines or Application Programme Interface (API) to flow real-time and read only view data into the HealthShare Instance environment to create an ICWR for the H&W Partners. 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 to enable Intersystem produce an aggregate data for a user.</p> <p>Care Plans: Part of the functions in ICWR is to enable health/care professionals to work with their patients/service users to create plans within the system which will be stored in the Operational Health Datastore. The solution is to have just one Care Plan for each patient/service user, which encompasses all the data required by the various clinical pathways that the patient/service user is on.</p> <p>If a health/care professional creates a Care Plan for a patient/service user and populates the plan (either from data they have entered in their own systems or by starting a care plan in ICWR) then if a health/care professional, in another organisation begins another Care Plan for a different care pathway, they will see</p>

that there is already an existing Care Plan in place for that patient/service user, that the core information is already populated and so they only have to add the data that is specific to their pathway's Care Plan.



Each health/care professional is responsible for the accuracy of the data that they input (including changes), therefore the organisation who employs the health/care professional for the care that they are recording will be the Controller.


Managing individual rights including (subject access requests):

As part of the InterSystems collaboration the Pan Midlands STPs (H&W STP, BSOL and Coventry and Warwick STPs) will work together to set up a central team that will be responsible for processing queries and requests under the data subject's rights. These include the right:


- To access, view or request copies of their personal information.
- Request rectification of any inaccuracy in their personal information.
- Raise an object to having their health and care record integrated
- 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.

3.4	What is the source of the data?	
	The source of the information shared in this way is electronic health or social care record held in each source system (e.g. EMIS, Adastral, Liquid Logic).	
3.5	Provide a list of the organisations/partners/stakeholders involved in sharing/processing of processing of personal/special categories personal data, and their roles (e.g. controller, processor, or joint controllers).	Are the organisations compliant with the Data Security and Protection (DSP) Toolkit?
	Name	Controller / Processor
	Worcestershire Acute Hospitals NHS Trust	Controller
	Herefordshire and Worcestershire Health and Care NHS Trust	Controller
	Wye Valley NHS Trust	Controller
	West Midlands Ambulance Service NHS Trust	Controller
	Worcestershire County Council	Controller
	Herefordshire Council	Controller
	Taurus Healthcare Limited, Herefordshire	Controller
	Practice Plus Group	Controller
		19/20 Standards Not Fully Met (Plan Agreed)
		19/20 Standards Not Fully Met (Plan Agreed)
		19/20 Standards Not Fully Met (Plan Agreed)
		19/20 Standards Met
		19/20 Standards Met
		19/20 Standards Met
		19/20 Standards Met

	St Richards Hospice, Worcester	Controller	TBC							
	Primrose Hospice, Bromsgrove	Controller	19/20 Standards Met							
	St Michael's Hospice Hereford	Controller	19/20 Standards Met							
	Wyre Forest, KEMP Hospice	Controller	19/20 Standards Met							
	GPs across Herefordshire and Worcestershire  List of H&W GP Practices.xlsx	Controllers	Yes							
	Herefordshire and Worcestershire Clinical Commissioning Group	Service Commissioner	In progress (new entity from 1 st April)							
	Intersystems	Processor (system supplier)	19/20 Standards Met							
<p>Any Partner that does not fully meet the DSPT standards by 2020-21 year will be required to adopt an alternative, but equivalent standard to the DSPT. This may include:</p> <ol style="list-style-type: none"> 1. Applying information security management and, quality assurance standards (ISO 27001 and 9001) and provide evidence of a Statement of Applicability or, 2. Ensure that it has in place documented IG policies, procedures and guidance that references confidentiality and data protection, information security and records management. 										
3.5.1	Will this information be shared/processed outside the organisations listed above in section 3.5									
	<i>If yes, describe who and why</i>									
	No									
3.6	What is the nature of the data, and does it include special category or criminal offence data?									
	A full list of dataset and data item (containing personal data, and special categories of personal data) that will be shared between the H&W health and care partners is embedded below:									
	 H&W ICWR Full Datasets_V3.docx									
	For the avoidance of doubt, data to be shared/processed is determined by the H&W STP Clinical and Professional Group.									
	Forename	Yes	Surname	Yes	Date of Birth	Yes	Age	Yes	Gender	Yes
	Address	Yes	Postal address	Yes	Employment records	No	Email address	Yes	Postcode	Yes
	Other unique identifier		Telephone number	Yes	National Insurance No	No	NHS No	Yes	Hospital ID no	Yes

	(please specify)								
	Other data (Please state):		E.g. Financial or credit card details; Local Gov. Identifier, CCTV or call recordings, or any unique identifier. (please specify)						
Special Categories of Personal Data									
Racial or ethnic origin			Yes	Political opinion		No	Religious or philosophical beliefs		No
Trade Union membership			No	Physical or mental health or condition				Yes	
Sexual life or sexual orientation		No	Social care assessment records (including care plans)		Yes	Safeguarding data (including child protection records)			Yes
Criminal conviction	No	Housing records	Yes	Safeguarding information		Yes	Assessment information		Yes
DNA profile	No	Fingerprints	No	Biometrics	No	Genetic data			No
	Other data (Please state):		E.g. Financial or credit card details; Local Gov. Identifier, CCTV or call recordings, or any unique identifier. (please specify)						
3.7	Is the data electronic, paper or both?								
	Electronic only								
3.8	How much data will be collected and used?								
	<p>The number of data that will be collected and used shall be determined by the number of data subjects registered/recorded in each health or social system (EMIS, Adastra Mosaic etc) and are accessing the health and/or social care service. Integrated Care and Wellbeing Record (ICWR) will cover patients/service users/clients living in the Herefordshire and Worcestershire with a population of 0.8 million.</p> <p>A full list of dataset and data item is embedded below:</p>								
	 <p>H&W ICWR Full Datasets_V3.docx</p>								
3.9	How often will be data be used (frequency)?								
	Data will be used daily for the purpose of Direct Care and Administration								
3.10	Data Retention Period								
	<i>How long will the data be kept?</i>								
	<p>The Partners / Controllers recognise that different record retention arrangements are needed in respect of retention and disposal schedules of personal, special categories of personal data. Therefore, the partners to the ICWR sharing shall adopt the procedure for archiving, retention and disposal of information set out in the Records Management Codes of Practice for Health and Social Care 2020</p>								

3.11	<p>How many individuals are affected?</p> <p>The number of patients/service users/clients whose personal data concerning health or social care processed for the purpose of direct care and administration shall be determined by the number of data subjects registered/recorded in each health or social system (EMIS, Aadastra Mosaic etc).</p>
3.12	<p>What geographical area does the use/sharing/processing cover?</p> <p>Integrated Care and Wellbeing Record (ICWR) will cover patients/service users/clients living in the Herefordshire and Worcestershire with a population of 0.8 million</p>
3.13	<p>What is the nature of your relationship with the individuals?</p> <p>Each Partner to the Herefordshire and Worcestershire ICWR provides either health or social care service to the individuals - patients/service users/clients for the purpose of direct care and administration. The individuals are therefore registered as either a patient/service users/client with each of the Herefordshire and Worcestershire health and care partners.</p>
3.14	<p>How much control will the individuals have?</p> <p>Each individual will have the right to:</p> <ul style="list-style-type: none"> • To access, view or request copies of their personal information. • Request rectification of any inaccuracy in their personal information. • Raise an object to having their health and care record integrated • Restrict the processing of their personal information where: <ul style="list-style-type: none"> ○ accuracy of the data is contested; ○ the processing is unlawful or, ○ where their data is no longer needed for the purposes of the processing. <p>Please see Step 7 for transparency and modalities</p>
3.15	<p>Would they expect you to use their data in this way?</p> <p>Yes.</p> <p>A fundamental element of the NHS Long Term Plan is the ability to deliver an Integrated health and care system that would enable health and care professionals share patients/service users/clients' information, to enable them make best informed decisions about individuals receiving health and/or care support.</p> <p>Integrated Care and Wellbeing Record (ICWR) would enable health and care professionals who are directly involved in a patient's care to access the information needed to provide that patient with the best possible care.</p>
3.16	<p>Do the individuals (data subject) include children or other vulnerable groups?</p> <p>Yes.</p> <p>Personal or special categories of personal data of children and/or vulnerable group is held in each health and/or social care source system.</p> <p>Children's information will be shared between registered and regulated health and/or social care professionals who are directly involved in their health/care to provide them with the possible service.</p> <p>Information about vulnerable group (children and adults) will be shared between registered and regulated health and/or social care professionals who are directly involved in their health/care in circumstances</p>

	relating to life or death or, where an individual is identified as being at risk from harm, and there is a duty to protect/safeguard that individual.
3.17	Are there prior concerns over this type of processing or security flaws?
	No
3.18	Is it novel in any way?
	No
3.19	What is the current state of technology/system you will be using?
	Please see below embedded diagram for the current state of technology/system that will be used for sharing information into the ICWR:  ICWR Data Flow_V5.pdf
3.20	Are there any current issues of public concern that you should factor in?
	None
3.21	Has your organisation signed up to any approved code of conduct or certification scheme (once any have been approved)?
	<i>Under the GDPR, trade associations and other representative bodies who are able to speak on behalf of a group of organisations can create may draw up “codes of conduct” that identify and address data protection issues that are important to their members, such as fair and transparent processing, pseudonymisation or the exercise of people’s rights. “Certification scheme” is a way for an organisation to demonstrate compliance with GDPR. Certification scheme criteria is approved by the ICO and can cover a specific issue or be more general.</i>
	No
3.22	What would the project/process/work stream you achieve?
	The Integrated Care and Wellbeing Record (ICWR) Herefordshire and Worcestershire (H&W) will join up local data from multiple electronic health and care systems in H&W to provide read-only view of a patient’s health and/or social care record via the secure Health and Social Care Network (HSCN). ICWR would enable health and care professionals who are directly involved in an individual’s health or care to access the information needed to provide that individual with the best possible care.
3.23	What is the intended effect on individuals?
	<ul style="list-style-type: none"> • Better outcomes and more efficient health social care delivery for patients/service users/client across Herefordshire and Worcestershire irrespective of technological or organisational boundaries. • Improved availability of data for health and care professionals to enable them to make more informed decisions about the health/care of their patients • Avoidance of duplicate investigations improving patient experience • Improved safety for patients and care professionals due to increased awareness of key patient information e.g. prescribed medications.
3.24	What are the benefits of the project/process/work stream?
	The primary benefits of H&W Integrated Care and Wellbeing Record (ICWR) are anticipated to be, but not limited to:

- Improved availability of data for health and care professionals to enable them to make more informed decisions about the health/care of their patients.
- avoidance of duplicate investigations improving patient experience.
- Improved safety for patients and care professionals due to increased awareness of key patient information e.g. prescribed medications.
- Improved the patient experience by minimising repeat questions and offering safer services
- Improved communication between services and reliability of referrals
- Reduction attendances/admissions by having awareness of pre-existing conditions and treatment plans.

Benefit and Case Study from other STPs:

The “Benefit Realisation Case” of another STP that have developed an integrated health and care record showed that the majority of clinicians wanted to be able to view data from beyond their own organisation saving time in retrieving vital information. This equates to 9,400 hours of clinical time saved per year.

Efficiency savings included reduction in paperwork, less missing paperwork and reduction in investigations ordered by preventing duplication. The costs of running their integrated health and care record system each year equated to 57p per patient/service user per year but the savings equated to at least 121p per patient/service user per year.

The reduction in referrals equated to an annual saving of £133k whilst ceasing using other systems saved approximately £500k per year. The significant referral avoidance from GPs was because they were able to view existing results and history that would otherwise not have been available to them.

An important finding was that clinicians felt that not only the relationship with patients was better but also better patient engagement. It was felt that patients were more confident in the level of care received, more engaged and happier that their information was available.

For avoidance of doubt, health and care organisations who are currently developing an integrated health and care record within their respective geographical areas have come together to create [INTEROPen](https://www.interopen.org/interoperability-case-studies/), an action group to accelerate the development of open standards for interoperability in the health and social care sector. More information on case studies can be found here: <https://www.interopen.org/interoperability-case-studies/>

4. Step 4: Consultation process

4.1 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?

The following groups in the H&W STP have been consulting each other and working together to deliver the ICWR programme objectives:

- **ICWR Programme Board** – has the overall accountability and responsibility for the ICWR programme, setting out local leadership and collaboration.
- **Communication and Engagement Group** – is responsible for developing robust communication materials (posters and leaflets) to inform individuals about the propose use of their personal data, the benefits, risks and, how the individuals can exercise their rights; stakeholders and public

engagements. The group works closely with the IG group to develop patients/service users/clients' communications materials.

- **Information Governance Working Group** – responsible for all data security and confidentiality matters relating to the ICWR programme and working closely within the Processor (Intersystems) to carry out due diligence and ensure that the Processor is meeting all its obligations.
- Clinical Professional Group – responsible for clinical safety of information and ensuring that appropriate codes are applied.

Step 5: Assess necessity and proportionality

5.1 What is the lawfulness of processing

In order for the sharing of the personal, and special categories of personal data to comply with UK GDPR Article 5 and [Section 86 of the 2018 Act](#), (principles of data protection) it must be fair, lawful and transparent, and must meet at least one of the Article 6 conditions as well as Article 9 (in the case of special categories of personal data). UK GDPR Article 22 [and section 14 of the 2018 Act](#) conditions must also be met where special categories of personal data are processed using automated individual decision-making, including profiling. Therefore, the processing of the Shared Personal Data is permitted under the following UK GDPR and the 2018 Act:

Grounds relied on under GDPR Article 6	Why the grounds are met
UK GDPR Article 6(1) (e) - 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.	The Partners to ICWR are statutorily constituted to provide health or social care services. Section 8 of the 2018 Act confirms that processing personal data for the purposes of performing a task in the public interest will include processing which is necessary for statutory functions. Therefore, it is necessary for each of the Partner to share/process personal data to fulfil their functions as statutory health and/or social care bodies.
Grounds relied on under GDPR Article 9	Why the grounds are met
UK GDPR Article 9 (2) (h) - processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of the domestic law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3 .	It is necessary for the Partners to share/process special categories of personal data concerning health for the purpose of Direct Care to provide a safe and effective system of healthcare to each individual patient/servicer user/client.
Provisions relied on under DPA Section 8	Why the grounds are met

<p>The lawfulness of sharing/processing of Personal Data set out in Article 6(1) (e) of the UK GDPR (as above) is permitted under Section 8 (d) of the 2018 Act:</p> <p>Processing is necessary for the exercise of statutory functions.</p>	<p>It is necessary for the Partners to share/process Personal Data under for the purposes of Direct Care to enable the Parties perform their statutory duties as providers of health and/or social care services.</p>
<p>Provisions relied on under DPA Section 10</p>	<p>Why the grounds are met</p>
<p>The lawfulness of sharing/processing of special categories of personal data set out in Article 9 (2) (h) of the UK GDPR (as above) is permitted under Section 10 of the 2018 Act (health and social care purposes)</p>	<p>The grounds for the sharing/processing meets the following provisions set out in Part 1, Schedule 1 (2) of the 2018 Act:</p> <p>Health or social care purposes means the purposes of:</p> <ul style="list-style-type: none"> a) preventive or occupational medicine; b) medical diagnosis; c) the provision of health care or treatment; d) the provision of social care, or the management of health care systems or services or social care systems or services.
<p>Provisions relied upon for obligation of professional secrecy</p>	<p>Why the grounds are met</p>
<p>For the purposes of Article 9(2) (h) of the UKGDPR, the circumstances in which the sharing/processing of special categories of personal data is carried out is subject to the conditions and safeguards referred to in Article 9(3) (obligation of professional secrecy). Therefore, in accordance with Section 11(1) of the 2018 Act, these will include circumstances in which it is carried out –</p> <ul style="list-style-type: none"> (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. 	<p>Access to special categories of personal data will be carried out by “registered and regulated” health or social care professionals (e.g. doctors, nurses social care professional), and non-registered professionals (e.g. receptionists) who owe a duty of confidentiality as a result of their employment by the health or social care organisation.</p> <p>The terms “health professional” and “social work professional” are defined in Section 204 of the 2018 Act, and include a broad range of different professionals.</p>
<p>The following lawfulness for process shall also apply in circumstances relating to life or death or, where an individual is identified as being at risk from harm, and there is a duty to protect/safeguard that individual:</p> <ul style="list-style-type: none"> • UK GDPR Article 9 (2) (c) – the processing is necessary to protect the vital interests of the data subject; 	

- [In accordance with Schedule 1, Part 3, \(30\) \(b\) of the 2018 Act - the conditions for protecting individual's vital interests is met where the data subject is physically or legally incapable of giving consent.](#)
- [In accordance with Schedule 1, Part 2 \(18\) \(1a\) of the 2018 Act - the conditions is met where the processing is necessary for protecting an individual from neglect or physical, mental or emotional harm, or protecting the physical, mental or emotional well-being of an individual](#)

Common Law Duty of Confidentiality

As the sharing/processing of personal data and special categories of personal data is for the purpose of Direct Care and Administration, a patient's consent to such shall fall under the Common Law Duty of Confidentiality and can be "**implied where is it informed**". Therefore, the Parties shall ensure that:

- (a) Their Privacy Notices are up to date and the nature of the sharing is actively communicated to patients/servicer users/clients
- (b) There are robust communication materials (posters and leaflets) to inform patients/service users about the propose use of their personal data, the benefits, risks and, how the patients/service users can exercise their rights.

[Paragraph 28 of the GMC Code Confidentiality](#) states that implied consent under the Common Law Duty of Confidentiality can be used if four conditions are met, these being:

- *28a: You are accessing the information to provide or support the individual patient's direct care or are satisfied that the person you are sharing the information with is accessing or receiving it for this purpose.*
- *28b: Information is readily available to patients, explaining how their information will be used and that they have the right to object. This can be provided in leaflets and poster, on websites and face to face. It should be tailored to patients' identified communication requirements as far as practicable.*
- *28c: You have no reason to believe the patient has objected.*
- *28d You are satisfied that anyone you disclose personal information to understands that you are giving it to them in confidence, which they must respect.*

The Health and Social Care (Safety and Quality) Act 2015 (Duty to Share)

[The Health and Social Care \(Safety and Quality\) Act 2015](#) inserted section 251A and B into the Health and Social Care Act 2012, which introduced a legal duty on health or adult social care commissioners and providers to share patient/service users' information where doing so will facilitate the provision of health services or adult social care to that individual, and where it is in the patient/service users' best interests.




This is not an unqualified duty, and health or adult social care organisations are not obliged to share information if they reasonably consider that one or more of the following may apply:



- If the patient/service user objects, or would be likely to object, to the disclosure of the information;
- the information concerns, or is connected with, the provision of health services or adult social care by an anonymous access provider; or
- for any other reason the relevant health or adult social care commissioner or provider is not reasonably able, or should not be required, to comply with the disclosure or, if the request would be inconsistent with—
 - (a) any provision made by or under the Data Protection Act 2018, the General Data Protection Regulation or the Law Enforcement Directive; or

	<p>(b) a Common Law Duty of Care or Confidence</p> <p>Accordingly, each Party shall ensure that it complies with this duty, taking care to ensure that they are fully aware of the limitations and exceptions to that duty.</p>	
	<p>Lawfulness for processing/sharing Staff personal data (which is contained within patient/service user/client's record)</p>	
	<p>Grounds relied on under GDPR Article 6</p>	<p>Why the grounds are met</p>
	<p>UK GDPR Article 6(1) (b) - processing is necessary for the performance of a contract to which the data subject is party.</p>	<p>Personal information and speciality of a health or care professional (staff) are included in a patient/service user's record to be able to identify the health/care professional (e.g. GP, Consultant or Social Care Professional etc) involved in the patient/service user's care therefore, it is necessary for each of ICWR Partner to share/process Staff Personal Data in order to fulfil their functions as statutory health and/or care bodies.</p>
5.2	<p>Does the processing actually achieve its intended purpose?</p>	
	<p>Yes</p>	
5.3	<p>Is there another way to achieve the same outcome?</p>	
	<p>No</p>	
5.4	<p>How will function creep be prevented?</p>	
	<p>Function creep will be prevented by regularly reviewing this DPIA, its processing, processes, supporting documentation, communicating materials and privacy information to ensure that the purpose of the processing have not evolved over time beyond those that are originally specified.</p>	
5.5	<p>How will you ensure data minimisation?</p>	
	<p>Personal and special categories of personal data shared for the purpose of ICWR (Direct Care and Administration) shall be:</p> <ul style="list-style-type: none"> • 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. <p>The ICWR 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 and those changes being made available to ICWR.</p> <p>User "access level" to ICWR shall be minimised and managed in line with the Role Based Access Control (RBAC) within the ICWR 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".</p> <p>Access shall be granted strictly on "need to know basis" in accordance with the 3rd data protection principle and 4th Caldicott Principle.</p>	
5.6	<p>Describe what steps are taken to ensure the quality of the data</p>	

	<p>The data to be shared/processed will reside in each Partner’s source system(s) which will be linked with other systems to create integrated electronic health and care record - ICWR. This means each partner organisation shall be responsible for the quality and accuracy of the data they agree to share, and controlling access to such data by creating a security group in active directory (or equivalent) to which relevant staff from the partner organisations will be added or removed in a timely manner.</p> <p>Each Partner organisation shall:</p> <ul style="list-style-type: none"> • Take all reasonable steps to ensure the quality and accuracy of data in its system(s) (with "accuracy" meaning that the data is correct, complete and up-to-date) which it is sharing and have in place appropriate systems to update any information if subsequently discovered to be inaccurate. • Inform the system supplier (InterSystems) and recipient Partners of that inaccuracy or omission, who will then take immediate steps to correct or remove the inaccurate information; and • consider whether to inform the Data Subject, of the inaccuracy or omission; <p>The system supplier (Intersystems) shall provide data quality and load reports throughout this process for downstream systems data.</p>
<p>5.7</p>	<p>What information will be given to individuals?</p> <p>Robust communication materials (posters, leaflets etc) on ICWR will be developed and will be made widely available at least eight weeks prior to ICWR go-live.</p> <p>Each Partner/Controller shall ensure that:</p> <ul style="list-style-type: none"> • The robust communication materials (e.g. posters and leaflets) are issued to individuals and visible in their organisation (paper and electronic) to inform patients/service users/clients about the propose use of their personal data, the benefits, risks and, how they can exercise their rights. • Its Privacy Notice is up to date and the nature of the sharing is actively communicated to patients/service users/clients. <p>A Privacy Notice covering ICWR information sharing/processing will be developed for organisations to use.</p>
<p>5.8</p>	<p>What measures are in place to ensure that processor/s (if any any) comply?</p> <p>The Processor will be required to:</p> <ul style="list-style-type: none"> • Demonstrate compliance with the Data Security and Protection Toolkit (DSPT) • Demonstrate compliance with security management and, quality assurance standards (ISO 27001 and 9001) and provide evidence of a Statement of Applicability. • Sign a Data Processing Agreement with the Controllers in accordance with GDPR Art. 28(3) • 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 in ICWR (for the purposes of maintenance and support) are appropriately vetted, and compliant with mandatory data security training. <p>The list is not exhaustive</p>
<p>5.9</p>	<p>How do you safeguard any international transfers?</p> <p>No personal will be transferred outside the UK</p>

Other data <i>(Please state):</i>	Please see full list of datasets embedded above
-----------------------------------	---

Step 6: Describe the responsibilities linked to the sharing / processing		
6.1	If you have answered 'yes' to 3.1, is there a documented Data Sharing Agreement (DSA) in place between the Controllers?	Yes/No
	<p><i>(if yes, please embed a copy of the DSA here)</i></p>  <p>Data Sharing Agreement_ICWR_re</p>	Yes
6.2	If there is a Processor involved, are the obligations of the Processor clearly set out in a Data Processing Contract/Agreement?	Yes/No
	<p><i>In accordance with GDPR Art. 28 processing by a Processor must be governed by a Data Processing Contract/Agreement which must be evidence in writing.</i></p> <p><i>(if yes, please embed a copy of the Data Processing Contract/Agreement here)</i></p> <p>As the Processor InterSystems will be storing/hold batch files in its data repository there is the need for a Data Processing Agreement between the Controllers and Processor (in progress).</p>  <p>Data Processing Agreement_HW CCC</p>	In progress
6.3	As part of this project is the use of Cloud technology being considered either by your own organisation or a 3rd party supplier/processor?	Yes/No
	<p>The Cloud Risk Assessment has been completed by IntersyStems and can be found in the following embedded attachment:</p>  <p>Cloud Hosting Risk Assessment_HealthS</p>	Yes
6.4	Does the project involve employing contractors external to the organisation who would have access to personal or special categories of personal data?	Yes/No
	<i>If yes, embed here, a copy of the confidentiality agreement or contract for 3rd Party Staff</i>	No
6.5	Do the Controllers and their representative(s) have Records of Processing Activities (RoPA) in place to underpin the sharing/processing?	
	<i>To demonstrate compliance with GDPR Art. 30 and DPA Section 61, the controller or processor shall maintain Records of Processing Activities (RoPA) under their responsibility. The RoPA shall contain the name and contact details of the</i>	

	<p>controller and, where applicable, the joint controller, the controller's representative and the data protection officer; the purposes of the processing; a description of the categories of data subjects and of the</p>
	<p>Yes – copy of RoPA is embedded below:</p> <p> Records of Processing Activities</p>
<p>6.6</p>	<p>Where the processing includes special categories of personal data, does the Controller(s) and their representative (processor) have an “Appropriate Policy Document” in place that explains the "safeguards" for processing those special categories of personal data?</p> <p><i>Part 1 of Schedule 1 (4) of DPA 2018 requires a Controller and a Processor to have an Appropriate Policy Document in place for processing relating to employment, social security and social protection, health or social care and public health purposes. The Policy should explain controller/processor's procedures for securing compliance with the principles relating to processing of special categories of personal data; explain the controller/processor's policies as regards the retention and erasure of special categories of personal data, and giving an indication of how long such data is likely to be retained.</i></p> <p>Each Controller (ICWR Partner) and the Processor (InterSystems) shall ensure that it has in place an Appropriate Policy Document that provides information about safeguards for shared special categories of personal data. A template from the Information Commissioner is embedded below for the parties to adopt (if not available):</p> <p> Appropriate-policy-document_ICO Tem</p>

<p>Step 7: Transparency and Modalities</p>	
<p>7.1</p>	<p>Have individuals been informed about the proposed use of their personal or special categories of personal data?</p> <p><i>For example, have the organisations/partners listed in section 3.1 updated Privacy Notice reflect ICWR information sharing?</i></p> <p>Robust communication materials (posters, leaflets etc) are being developed and will be made widely available at least eight weeks prior to ICWR go-live.</p> <p>Each Partner/Controller shall ensure that:</p> <ul style="list-style-type: none"> • Its Privacy Notice is up to date and the nature of the sharing is actively communicated to patients. • The robust communication materials (e.g. posters and leaflets) are visible in their organisation (paper and electronic) to inform patients/service users/clients about the propose use of their personal data, the benefits, risks and, how they can exercise their rights. <p>A Privacy Notice covering ICWR information sharing/processing will be developed for organisations to use.</p>
<p>7.2</p>	<p>How can data subjects exercise their rights to access, view or request copies of their personal data?</p>

	<p>As part of the InterSystems collaboration the Pan Midlands STPs (H&W STP, BSOL and Coventry and Warwick STPs) will work together to set up a central team that will be responsible for processing queries and requests under the data subject's rights. This includes the right:</p> <p>To access, view or request copies of their personal information. Data subjects will also be able to exercise their right by contacting their relevant health provider. Contact addresses shall be provided in communications materials such as posters, leaflets and on each Controller's Privacy Notices.</p>
7.3	<p>How can data subjects exercise their rights to request rectification of any inaccuracy in their personal data?</p> <p>As part of the InterSystems collaboration the Pan Midlands STPs (H&W STP, BSOL and Coventry and Warwick STPs) will work together to set up a central team that will be responsible for processing queries and requests under the data subject's rights. This includes the right to:</p> <ul style="list-style-type: none"> Request rectification of any inaccuracy in their personal information. <p>Data subjects will also be able to exercise their right by contacting their relevant health provider. Contact addresses shall be provided in communications materials such as posters, leaflets and on each Controller's Privacy Notices.</p>
7.4	<p>How can data subjects exercise their rights to erasure ('right to be forgotten')?</p> <p>Under the data protection legislation, a data subject has a right to erasure (right to be forgotten) where he/she had given 'consent' to the processing of his/her personal data and later withdrew that consent. As the data being shared is for health or social care purposes, a right to erasure (right to be forgotten) does not apply given the processing is necessary for:</p> <p><i>for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services.</i> Article 9 (2) (h)</p>
7.5	<p>How can data subjects exercise their rights to restrict the processing of their personal data?</p> <p>As part of the InterSystems collaboration the Pan Midlands STPs (H&W STP, BSOL and Coventry and Warwick STPs) will work together to set up a central team that will be responsible for processing queries and requests under the data subject's rights. This includes the right:</p> <ul style="list-style-type: none"> To restrict the processing of their personal information where: <ul style="list-style-type: none"> accuracy of the data is contested; the processing is unlawful or, <p>where their data is no longer needed for the purposes of the processing.</p>
7.6	<p>How can data subjects exercise their rights to data portability?</p> <p>The data subject shall have right to data portability by contacting the relevant health or social care provider to request the data which they provided to the health provider/Controller (not data generated by the Controller) in a structured, commonly used machine readable format. For the avoidance of doubt, right to portability does not apply to ICWR processing/sharing because:</p> <ul style="list-style-type: none"> data is not processed by automated means;

	<ul style="list-style-type: none"> consent and contract fulfilment are not the legal bases for the processing/sharing <p>The Controllers shall have a robust Subject Access Policy in place to ensure the rights of the individual to access data are handled in line with legislative requirements</p>
7.7	<p>How can data subjects exercise their rights to object to the sharing/processing of their personal data?</p> <p>As part of the InterSystems collaboration the Pan Midlands STPs (H&W STP, BSOL and Coventry and Warwick STPs) will work together to set up a central team that will be responsible for processing queries and requests under the data subject’s rights. This includes the right:</p> <ul style="list-style-type: none"> To raise an object to having their health and care record integrated <p>In line with UK GDPR Article 21 and DPA Section 99 of the 2018 Act, the data subject has a general right to raise an objection to the processing of their personal data and they also do so by contacting their health provider relevant health provider. Contact addresses shall be provided in communications materials such as posters, leaflets and on each Controller’s Privacy Notices.</p> <p>Relevant Code of Practice and Legislation:</p> <ol style="list-style-type: none"> National Data Guardian Report of 2016 (see clause 3.2.12 of page 26) states: <i>A person can still ask for their health care professional not to share a particular piece of information with others involved in providing their care. This may be in relation to a local shared record programme. Local communication materials should inform people what they should do if they have concerns.</i> The ICO’s guidance on lawfulness for processing under Article 6(1)(e) – public task, states: an individual need to be given the “right to object” when their personal data is processed for “public task” purposes – GDPR Art. 6(1)(e). “Public task” is one of the legal basis for integrated/electronically linked health record. Paragraph 4(a) of section 251B of the Health and Social Care (Safety and Quality) Act 2015 (Duty to Share) states a patient has the right to object to having their health and care record shared with the other health and care organisations. <p>Data subjects’ right to raise an object to have an integrated electronic record linkage shall be set out in the communication materials (privacy notices, posters and leaflets) and the benefits and risks shall be explained.</p>
7.8	<p>Will the processing of data include automated individual decision-making, including profiling?</p> <p><i>If yes, please outline the profiling processes, the legal basis underpinning the process, and the rights of the data subject</i></p> <p>No</p>
7.9	<p>Will individuals be asked for consent for their information to be processed/shared?</p> <p><i>If no, list the reason for not gaining consent e.g. relying on other lawful basis, consent is implied where it is informed.</i></p> <p>No – Consent is not the legal basis for processing.</p>
Step 8: Information Security and Supporting Assets	
8.1	<p>Describe the process in place for auditing access to personal data</p> <p>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.</p>

The Processor – Intersystems shall use ‘user access authentication’ mechanisms to ensure that all instances of access to any Personal Data in the ICWR 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 and ICWR environment:

- The system can track and audit all user access, including who, when, where and what was accessed, including data subject’s record access 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 be 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.

In addition, each Partner will be required to audit access to the ICWR and report any anomalies to the other Parties and Intersystems.

8.2	Describe the Role Based Access Control (RBAC) within the system how access to information be controlled
	<p>Role Based Access Control (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.</p> <p>Access to the Integrated health and care 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 dependent on the technical set up at each organisation.</p> <p>There are two main types 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:</p> <ul style="list-style-type: none"> • 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). <p>Depending on the STP’s preference for ICWR, the system has the functionality to split the above job roles into the following RBAC matrix:</p>

	<u>Level 1 Admin</u>	<u>Level 2 Support</u>	<u>Level 3A Clinical</u>	<u>Level 3B Medical / Clinicians</u>	<u>Level 4 System Admin</u>	
	<ul style="list-style-type: none"> • Receptionist • Clerical • Ward Clerk 	<ul style="list-style-type: none"> • Clinical Admin • Student Nurses • Student Midwives • Student AHPs • Social Worker • Allied Health Professional • Advanced HCA • Medical Secretary • Physiotherapist 	<ul style="list-style-type: none"> • Medical Admin • Care Navigators • Speech Therapist • Clinical Psychologist • Physiotherapist (MDT/ESP) • ASC Clinical Worker • Records Manager • Health Visitor • Practice Manager • District Nurse • Pharmacists 	<ul style="list-style-type: none"> • Consultants • Doctors • Matrons • Nurses • GPs 	<ul style="list-style-type: none"> • System Administrator Registry • System Manager • Tech Support 	
	<p>Where a user in an organisation is requesting data of a patient/service user/client the system performs the following steps:</p> <ul style="list-style-type: none"> • Confirms the role of the requestor and whether they can place the request • Approved request is sent via the Gateway to the source system • Source system pushes the data to the Gateway • Gateway checks the data and rejects data that will not be forwarded based on the role of the requestor and whether the data source contains sensitive/opt-out data record • Requestor views the data on their device <p>For the avoidance doubt, the Collaborative Care Record Oversight Authority (CCROA) which BSOL and H&W BSOL STP are working together to agree an RBAC matrix as the parties on same instance/platform of Intersystems.</p>					
8.3	What roles will have access to the information? (include a list individuals or staff group)					
	<p>As above, there are two main types 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:</p> <ul style="list-style-type: none"> • Application level roles – e.g. Clinicians, Social Care Professionals, Admin-Clerical Staff, etc. • Database level roles – e.g. “Database Administrator”, “Interface Developer, security configuration etc (system maintenance purposes). <p>Depending on the STP’s preference for ICWR, the system has the functionality to split the above job roles into the above RBAC matrix:</p> <p>Access roles be determined by the Collaborative Care Record Oversight Authority (CCROA) which BSOL and H&W BSOL STP are working together to agree an RBAC matrix as the parties on same instance/platform of Intersystems. Such access is granted on a strict ‘Need to Know’ basis and managed in line with the access rights that the health/care professional has within their source system.</p>					
8.4	What security and audit measures have been implemented to secure access to and limit use of personal data and/or special categories of personal data?					
	Username and password	X	Smartcard	X	Firewalls / VPN / Encryption Cert.	X

	System audit	X	Restricted access to Network Files	X
	Other: <i>Provide a Description Below:</i>			
	Role Based Access Control (RBAC)			
8.5	<p>Is there a documented Information Security Management Plan (ISMP) or System Level Security Policy (SLSP) in place for this project/system? If yes, please embed a copy below.</p> <p><i>SLSP refers to the architecture, policy and processes that ensure data and system security on individual computer systems. It facilitates the security of standalone and/or network computer systems/servers from events and processes that can exploit or violate its security or stature.</i></p> <p>The Intersystems Information Security Management Plan has been provided here in its generic form – at the point of contract signature, we would localize this to the customer’s needs. This also contains reference to the BCP below.</p>  <p>ISC UKI ISMP Template.pdf</p>			
8.6	<p>Is there a Business Continuity Plan (BCP) or Disaster Recovery Protocol for the proposed/existing system or process?</p> <p><i>If yes, please embed a copy below, and give reference to such plan and protocol.</i></p>  <p>UKI Business Continuity Plan Overv</p> <p>This plan defines how ISC invoke their Business continuity plan and disaster recovery. Supporting this there must similarly be a process defined by the Herefordshire and Worcestershire STP of how a business continuity is to be communicated and acted upon e.g. alternative data sources.</p>			
8.7	<p>What are the data supporting assets?</p> <p>List the data supporting assets (operating systems, business applications, database management systems, office suites, protocols, configurations, etc.)</p>			
8.8	<ul style="list-style-type: none"> • Smartcard – RBAC • Network PCs, laptops (encrypted) • Enterprise Master Patient Index (EMPI) • HCSN network connection • Secure servers • Firewalls • Security patching • Anti-virus protection • Secure file transfer protocol (SFTP) • Integration engines • Data warehouse 			

8.9	Is Mandatory Staff Training in place for the following?	Yes/No	Dates
	<ul style="list-style-type: none"> Use of the System or Service: 	Yes	Intersystems demonstration is holding on 17 th and 18 th December 2020
	<ul style="list-style-type: none"> Data Security Training 	Yes	Each partner organisation is responsible for ensuring that their staff are compliant with their mandatory data security training
8.10	Are there any new or additional reporting requirements for this project?	Yes	
	<ul style="list-style-type: none"> What roles will be able to run reports? 		
	By way of service contract/SLA, IntersyStems' staff (e.g. database administrators, developers, security configurators and analysts) will be required to run reports for the following purposes:		
	<ul style="list-style-type: none"> System audit to ensure that all instances of access to any Personal Data in ICWR are auditable against an individual. System maintenance support 		
	Will the reports contain person, and/special categories of personal data or, pseudonymised or anonymised format?		
Personal data – first name and last name of a user			
8.11	Have any confidentiality and data security risks been identified relating to this project? <i>(if Yes, the final section will need to be completed).</i>	Yes/No	

Step 9: Identify and Assess Risks			
Risk	Likelihood of occurrence	Severity of harm	Overall risk
Risk 1: Potential risk of inappropriate use/access of personal information by staff in partner organisations.	2	3	6
Risk 2: Noncompliance with the DSPT by partner organisations	2	2	4

Step 10: Identify Measures to reduce risk			
Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 9			

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
Risk 1	Mitigation Partner organisations must ensure that user access to ICWR is minimised and managed in line with the Role Based Access Control (RBAC) within their source systems. Access to personal data must be granted by each partner organisation to their staff/users strictly on need-to-know basis and the staff must only see the information they are required to enable them perform their roles.	Reduced	N/A	Yes
Risk 2	Mitigations Each Partner must ensure it has in place documented IG policies, procedures and guidance that references confidentiality and data protection, information security and records management. Partners who have not yet met the required DSPT standards Partners will be required to sign an Assurance Statement that sets out the process/action plan they will put in place to achieve the DSPT standards.	Reduced	N/A	Yes

Step 11: Sign off and record outcomes

Item	Name/date	Notes
Measures approved by:	SIRO	
Residual risks approved by:	SIRO	<i>Notes: If accepting any residual high risk, consult the ICO before going ahead.</i> Not Applicable. The risks are low therefore, they do not necessitate a consultation with the ICO
DPO advice provided:	The review and mitigating measures that have been put place show that the information sharing for the ICWR can proceed	<i>Notes: DPO should advise on compliance, step 10 measures and whether processing can proceed</i>

Summary of DPO advice:

Appropriate technical organisation security measures are in place within ICWR For example:

Role Based Access Control (RBAC).

<p>Audit controls: The Processor – Intersystems shall use ‘user access authentication’ mechanisms to ensure that all instances of access to any Personal Data in the ICWR 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:</p> <ul style="list-style-type: none"> • 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; 		
DPO advice accepted or overruled by:	Accepted	<i>If overruled, you must explain your reasons</i>
<p>Comments: Not applicable</p>		
Consultation responses reviewed by:	The SIRO has consulted with the DPO on the risks identified above and their decisions to mitigate and accept the above risks do not depart	<i>If your decision departs from individuals’ views, you must explain your reasons</i>
<p>Comments: No further comments</p>		
This DPIA will kept under review by:	DPO	<i>The DPO should also review ongoing compliance with DPIA</i>
Signature: D Burrell	Print name: David Burrell CEO	

Glossary of terms

1. Personal data' means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
2. Special Categories of Personal Data mean data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.
3. Controller' - means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.
4. Processor - means a natural or legal person, public authority, agency or other body which processes personal data on behalf of a Controller.
5. Processing' - means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
6. *Data Subject* – an individual who is the subject of personal information.
7. *Direct Care* - means clinical, social or public health activity concerned with the prevention, investigation and treatment of illness and the alleviation of suffering of individuals (all activities that directly contribute to the diagnosis, care and treatment of an individual).
8. Data Flow Mapping (DFM) means the process of documenting the flows/transfers of Personal Data, Sensitive Personal Data (known as special categories personal data under GDPR) and Commercially Confidential Information from one location to another and the method by which they flow.
9. Pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.
10. *Anonymised Data* - means data in a form where the identity of the individual cannot be recognised i.e. when:
 - Reference to any data item that could lead to an individual being identified has been removed;
 - The data cannot be combined with any data sources held by a Partner with access to it to produce personal identifiable data.

