One Health and Care

Shared Care Record

Data Protection Impact Report

Title: Shared Care Record (formally Integrated Care Record) – Data Protection Impact Assessment

Product: Graphnet and System C Alliance - CareCentric

Document Owner: OHC Information Governance Advisory Group

Date Created: 16 July 2019

Version History:

Version	Date	Updated By	Amendment/s
0.1	**16/07/2019**	**Hedda Motherwell**	First draft
0.2	**10/09/2019**	**Hedda Motherwell**	Updates due to project progress
0.3	**17/09/2019**	**Hedda Motherwell**	Updates due to project progress
0.4	**27/09/2019**	**Hedda Motherwell**	Risk Analysis updated
0.5	**07/11/2019**	**Hedda Motherwell**	Updates to S2.4.2 and Risk Analysis
0.6	**12/12/2019**	**Hedda Motherwell**	Exclusions appendix updated
0.7	**06/01/2020**	**Hedda Motherwell**	Updates throughout to reflect project progress
0.8	**20/01/2020**	**Hedda Motherwell**	Update to 2.4.2 – Access and Governance and Risk Analysis and risk score added. Fair Processing appendix.
0.9	**23/01/2020**	**Hedda Motherwell**	Update to Section 2.4.2 - Availability
0.10	**18/05/2020**	**Hedda Motherwell**	Updated throughout to reflect change to Opt Out approach Amendment to sign off page 2
0.11	**13/06/2020**	**Hedda Motherwell**	Update throughout to reflect change to Support Model and outstanding actions Section 4.
0.12	**03/09/2020**	**Hedda Motherwell**	Update throughout to reflect Personal Health Record and e-appointment aspects. Vocare Ltd details updated in section 1.7.
0.14	**09/11/2020**	**Hedda Motherwell**	Update throughout to reflect changes to PHR – Personal Health Record and access.
0.15	**02/03/2021**	**Hedda Motherwell**	DPIA amended to reflect an overarching One Health and Care DPIA - Updated throughout to reflect OHC DPIA rather than locality specific, to aid wider regional sign up to one overarching OHC DPIA - Partner sign off clarity expanded on page 2 - Full risk analysis removed into separate document specific for Staffordshire & SoT - To reflect system now being live Section 1.3 Assumptions removed and general tweaks throughout to language to reflect present tense - 2.5 Statutes and Key Areas for Consideration moved into Appendices - Appendix A – Parties removed: the ISA can be consulted for a full list of up to date OHC parties. - Schedule 1 updated with data flow diagrams and clarity around access.
0.16	**16/4/21**	**Lynnette Nott**	Shropshire data flows added to section 3
0.17	**06/05/21**	**Hedda Motherwell** **Lynnette Nott**	Following review by Information Governance Advisory Group 04/05/21: Update to Section 2.3 Scope - All data available within One Health and Care including any PHR data added by individuals will be replicated into the Business Analytics warehouse, any processing will only be for direct patient care. Page 21 Confidentiality and Integrity (Security) - Graphnet are obligated to adhere to all standards required and will be in breach of contract should the standards not be met. Page 31 Section 4 - Any information added to the app will then be available for data analysis under secondary use purposes, but not directly available for healthcare teams to view. It will only be used for secondary use purposes once a separate DPIA has been completed and approved
0.18	**13/5/21**	**Lynnette Nott**	SaTH update clinical system to include Semi Helix
1.0	**27/05/2021**	**Hedda Motherwell**	Reference to Opt out removed in Appendix D and doc finalised
2.0	**11/11/2021**	**Helen Butler**	Updated to reference terminology change from integrated Care record (ICR) to Shared Care Record (ShCR), Inclusion of Children's Social Care Data Feed, West Midlands ShCR, legislation updates. -1.4 Abbreviations, reference to ICS and ShCR added p 8 -2.3 reference to West Midlands Shared Care Record and three ICS regions p10 -2.4.1 Reference Joint Controller status p.10 -2.4.2 Additional legal basis referenced p.11 -p14 inclusion of handling objections for patients without listed GP - updated reference to Records Management code of practice 2021 p 18 - Section 3 Data Flows. 3.2.4 table removed amalgamated with table 3.2.1 organisations whose data feeds in near real time. 3.2.5 table removed amalgamated with table 3.2.5 organisations data feeds at least every 24 hours - Appendix D statutes p.44 reference to Children Act 1989/2004 statute for inclusion of Children's social care data.

Partner Organisation Sign Off

This document has been developed in consultation with the OHC Information Governance Advisory Group. It is an evolving document which will be regularly refreshed and developed as the programme of work continues. Significant amendments to the document will be outlined and approved by the Group.

Sign off of the OHC Data Protection Impact Assessment will be managed through the OHC Information Governance Advisory Group and recorded in minutes or through positive confirmation by email. By emailing it will be confirming that the relevant representative/s have read and have had opportunity to collaborate and contribute to this Data Protection Impact Assessment.

Risks and mitigating factors are documented and managed by individual partners of One Health and Care and will be fed into the OHC Information Governance Advisory Group when applicable. Identified risks will be managed by each organisations Data Protection Officer/Caldicott Guardian/SIRO, and through the partners internal processes.

Contents

1. Introduction

1.1 Background Information

The purpose of this document is to ensure that the One Health and Care Shared Care Record (OHC) is implemented with consideration of privacy laws compliancy. The document helps to identify, understand and manage or mitigate any privacy risks while allowing the aims of the project to be met.

Privacy risk is the risk of harm through an intrusion into privacy. This could be brought about by a breach of confidentiality and includes both the risk to an individual and organisational risk brought about from non-compliance with legal obligations and in turn reputational harm.

Individuals have the right to confidentiality and privacy and expect professionals to keep their data safe and secure. Clinicians and care providers also have a legal duty and professional obligation to respect privacy and keep information confidential in the course of care delivery. Therefore there must be a lawful basis to process service user data.

'Lawful' means there is a basis in law for the activity to be carried out and that it is done in compliance with various regulatory requirements regarding sharing information. UK General Data Protection Regulation (GDPR) and Data Protection Act 2018 (DPA) are currently the principle statutes regulating the sharing of information. As a general rule, if the sharing activity has an identified legal gateway and complies with data protection legislation it will be lawful.

The common law duty of confidence and Article 8 of the European Convention of Human Rights (a right to respect for a private life) also need to be taken into account.

This document has been developed in line with the Information Commissioners Conducting Privacy Impact Assessment Code of Practice.[1]

1.2 Expected Benefits of OHC

The business case presents qualitative and quantified benefits including:

- Potential reductions in acute activity of over £13M across 5 years for a cohort of just 2,000 patients with long term conditions. [Evidenced in Manchester through deployment of a Graphnet solution and based on PbR payment mechanisms]
- Potential reduction in administration resources within GP Practices of up to £400K (£2,600 per practice) per year by ensuring that providers use ICR for patient queries. [Evidenced in Sutton through deployment of a Graphnet solution]
- Reduced length of stay of between 0.5 and 3 days [average 1.7] across all non-elective admissions offering savings of £7.5M per year. This is achieved by using the available information, including previous diagnostics, to ensure that patients are on the most appropriate care pathway as soon as possible. [Evidenced in Hampshire through deployment of a Graphnet solution]
- System wide alerting to ensure that all appropriate alerts are shared between health and care professionals. Thereby offering a range of benefits from improved staff safety through to ultimately savings lives.

[1] https://ico.org.uk/media/for-organisations/documents/1595/DPIA-code-of-practice.pdf

- Enhancement of population health when tools and analytical processes are “plugged in” to the data to derive further intelligence and advanced intervention.
- Electronic Patient Appointments to substantially reduce DNAs and to put patients in control of their own appointments.[2]

1.3 Definitions

Data Controller	Determines the purpose and means of the processing of personal data.
Data Processor	Processes data on behalf of, and only under the instruction of, the Data Controller.
Data Protection Register	Under Data Protection legislation organisations that process personal data must pay a data protection fee to the Information Commissioners Office (ICO) (unless they are exempt from doing so). The ICO keep a register of all Data Controllers and how they process personal data.
Data Subject	The individual to which the personal data relates to.
Data Security and Protection (DSP) Toolkit.	Replaced the Information Governance Toolkit (IG Toolkit). It is an online self audit tool which consists of a framework for assuring that organisations are implementing the ten data security standards and meeting their statutory obligations on data protection and data security.
Direct Care	Clinical, social or public health activity concerned with the prevention, investigation and treatment of illness of an individual. The professional and their team have a legitimate relationship for the service users care and would be seen as the ‘direct care team’. It includes supporting a service users ability to function and improve their participation in life and society.
Explicit Consent	Any freely given, specific, informed and unambiguous indication of the data subject’s wishes by a statement or by a clear affirmation action, signifies agreement to the processing of personal data relating to him or her.
Implied Consent	Consent will be assumed unless the subject takes action to inform or register their objection. For example silence or inaction would be acceptable with Implied Consent. This is the basis for sharing under the common law duty of confidentiality. It is not recognised under data protection legislation.
Indirect Care	Activities which contribute to the overall provision of services to a population as a whole. This includes linked data used for running the health and social care systems and improving safety and quality of care, risk stratification, preventative medicine, health service management and medical research.
Information Governance Toolkit	The Information Governance Toolkit was a Department of Health (DH) Policy delivery vehicle that NHS Digital is commissioned to develop and maintain. It draws together the legal rules and central guidance set out by DH policy and presents them in in a single standard as a set of information governance requirements. Please see DSP Toolkit.
Information Sharing Agreement	Data Sharing Agreement and Information Sharing Agreement are one in the same, the terminology is used interchangeably across the OHC partners.
Partner	Throughout this document this term will be used for the organisations which are involved in the ShCR in terms of providing and/or viewing data within the system.

[2] ICR2 Full Business Cases v2.6.2, Page 9 - 10

Personal Health Record (PHR)	A secure, online record which stores information about a person's health, care and wellbeing. They are also sometimes referred to as Patient Portals or Patient Held Record.
Processing	Any operation or set of operations which is performed which is performed on 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.
Recipient	Natural or legal person, public authority, agency or another body to which personal data is disclosed.
Restrict processing	The marking of stored personal data with the aim of limiting the processing in the future. Under GDPR Data Subjects have the right under some circumstances to restrict the processing.
Third Party	Natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.
Service user	Throughout this document this term will be used as a capture all for all individuals who use the services of the partners involved in the ShCR.
Special Category	Personal 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. Formally known as 'sensitive personal data'.

1.4 Abbreviations

CCG	Clinical Commissioning Group
CESG	Communications Electronic Security Group
CSU	Commissioning Support Unit
DPA	Data Protection Act 2018
DPIA	Data Protection Impact Assessment
GDPR	UK General Data Protection Regulation
GP	General Practitioner
ICO	Information Commissioners Office
ICR	Integrated Care Record
ISA	Information Sharing Agreement
ICS	Integrated Care System
OHC	One Health and Care
ShCR	Shared Care Record

1.5 DPIA Development and Related Projects

There are future phases of OHC and linked projects which will require future iterations of this document or related DPIAs to be development. These include:

- Coordinated care plans – including data flows and process, data controller/ownership implications
- Secondary use of data, including business intelligence
- Patient Health Record (PHR) portal
- E-appointments

2. Data Protection Impact Assessment

2.1 Requirement

Data Protection legislation[3] makes it mandatory to perform a Data Protection Impact Assessment (DPIA) in case of large scale processing of special category data (for example health data). The identification of a legal basis is also needed before you start processing data; therefore a DPIA is required and should document the legal basis to be relied upon.

Conducting a DPIA helps to identify, understand and manage any privacy risks which relate to data whilst allowing a project to progress to meet its aims. The DPIA allows analysis of information rights law relating to a new system or process. The purpose of a DPIA is not to completely eliminate any impact on privacy but to ensure it is at an acceptable level and 'to consider whether the impact on privacy is proportionate to the aims of the project.'[4]

In order to establish when a DPIA is required a number of screening questions are needed, these are outlined below and are taken from the Information Commissioners Conducting Data Privacy Impact Assessment Code of Practice. If the response is 'yes' to any of the questions then a DPIA is required.

2.2 Screening Questions

	Yes/No	Comments
1. Will the project involve the collection of new information about individuals?	No	The project will not involve collecting new information however the project will involve the combining, matching and sharing of information to create a new holistic view of Data Subjects which will be new. Personal Health Record aspect involves individuals adding information themselves, only viewable by themselves.
2. Will the project compel individuals to provide information about themselves?	Yes	Personal Health Record element of the ShCR will provide the option for data subjects to add information regarding themselves. This information will then consequently be stored within the ShCR but may not be viewable.
3. Will information about individuals be disclosed to organisations or people who have not previously had routine access to the information?	Yes	The purpose of the ShCR is to share identifiable service user data between the partners of the project. The types of individuals (i.e. health and social care professionals) accessing the data will not change but the scope of available data and location of those professionals may change. Currently, the information that will be shared would be made available to these professionals on request. The ShCR speeds and simplifies the process but it does mean that records will be available to identified professionals without a more lengthy request procedure.

[3] GDPR, Article 35 (recitals 84, 89, 90, 91, 92, 93 and 95)

[4] Conducting Privacy Impact Assessments Code of Practice, 20140225, v1.0, Information Commissioner's Office. https://ico.org.uk/media/for---organisations/documents/1595/DPIA---code---of---practice.pdf

		Data Subjects will be informed of these changes through Fair Processing and in information given to Data Subjects at time of data collection.
4. Are you using information about individuals for a purpose it is not currently used for or in a way it is not currently used?	No	The data is collected by individual Data Controllers currently for Direct Care purposes. The purpose of the ShCR is for Direct Care. Data added by data subjects themselves via Personal Health Record element would be for direct care purposes.
5. Does the project involve you using new technology which might be perceived as being privacy intrusive? E.g. Use of biometrics or facial recognition?	Yes	The Personal Health Record aspect of the ShCR will have the ability for individuals to allow information from there 'wearables' such as FitBit to be uploaded to the ShCR.
6. Will the project result in you making decisions or taking action against individuals in ways which can have a significant impact on them?	No	Services and decisions made will be as previously for Direct Care purpose.
7. Is the information about individuals likely to raise privacy concerns or expectations? E.g. Health records, criminal records or other information that people would consider particularly private?	Yes	The information processed about service users relates to the activity undertaken by a health or social care professional in a care setting. Each 'case' will consist of a NHS number, organisation codes of the care providers, information about the event (date, admission reason, care provision etc.) and basic associated diagnosis, care pathway and procedure information. This represents full Personal Confidential Data (PCD) as defined in the Caldicott 2 Review[5] and as such is processing as defined by data protection legislation.
8. Will the project require you to contact individuals in ways which they may find intrusive?	No	

2.3 Scope

Patient information will be extracted from GPs and service provider systems such as acute hospital, social services, mental health and community (referred to in this document as 'partners'). This data is linked and will then form the Shared Care Record. The proposed legal basis which is outlined in this paper is based upon sharing patient level data through a Shared Care Record for the purposes of Direct Care only. Business intelligence, analytics, risk stratification and use by NHS Commissioners to inform other operational decisions for example is deemed a different purpose and will be covered by a separate DPIA.

Personal Health Record (including the e-appointments functionality) remains under the overarching purpose of Direct Care. Personal Health Record refers to the service user facing interface accessed through NHS App, One Health and Care refers to the clinician/professional facing interface. Both rely on the same data feeds from partners.

5 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf

All data available within One Health and Care including any PHR data added by individuals will be replicated into the Business Analytics warehouse, any processing will only be for direct patient care.

No Third Party will have access to the data at any point as a result of the OHC , unless outlined in the Information Sharing Agreement or a relevant Data Processing Agreement/overarching contract.

One Health and Care is not a national system, data will be shared by partners across three ICS boundaries

- Staffordshire and Stoke-on-Trent
- Shropshire, Telford and Wrekin
- Black Country and West Birmingham

A future intention is for the OHC to feed into the wider West Midlands ShCR program and participating organisations. The West Midlands ShCR programme will be documented in a separate DPIA and ISA.

2.4 GDPR Compliance

2.4.1 Joint Data Controller/ Data Controller/Data Processor

Under Data Protection legislation both Data Controllers and Processors can be liable for any breach of the regulation. The Controller determines the purpose, the Processor will carry out tasks on behalf of the Controller, under instruction and contract. If a breach occurs at the fault of the Processor outside of the remit of the contract the Processor would be liable.

Date Controller as defined by GDPR:

> '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'.

Joint Data Controller as defined by article 26 UK GDPR:

> 'Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers.'

Data Processor as defined by GDPR:

> 'a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller'.

When contracting the services of a Data Processor the following measures must be put into place:

- Defining who the Data Controller(s) and Data Processor(s) are
- Ensuring there is a robust written contract in place between DC and DP, including GDPR Article 28 requirements.

Breaches due to having no suitable contract in place between Data Controllers and Data Processors could see fines of up to £10 million for organisations. Under the DPA often the original cause of the breach instigates the fine and then the failure to have a suitable contract in place escalates the value. Failure to address any risks identified within the DPIA is not an option. Ineffective or weak IG controls in one organisation present a risk to the whole shared record community.[6] The OHC IG Steering Group will be responsible awareness and overview of risks, mitigating factors should be considered by the Group and put into place by the partner organisations where applicable.

In order for the ShCR to function the partner organisations process the data from a common pool and will be processing personal data for medical and related care purposes. Partner organisations will decide on the precise purpose and manner for which personal data is processed within the ShCR as Joint Data Controllers. Within the contractual terms each partner then determines how the data is used within their own organisation without the control of another body, thereby defining them each as Data Controllers in their own right.

The Data Processor is the System C and Graphnet Care Alliance; CareCentric system suppliers. They operate the technical support required thereby processing data on behalf of the Data Controllers under the overarching contract which reflects the content of a Data Processing Agreement. The system will be hosted by Microsoft Azure Cloud Computing Platform and Services, as subcontracted by System C and Graphnet Care Alliance. The Data Processor will not sub contract without written authorisation and assessment by the Data Controllers (as outlined within the overarching contract). The supplier will be required to provide assurance in regards to compliance with the Data Security and Protection Toolkit, Cyber Essentials Plus and ISO270001.

System C Healthcare Ltd (Data Processor) **and Microsoft Corporation (Microsoft Azure**) (Sub-processor) – hosting provision.

Graphnet Health Ltd (Sub-processor) – for implementation and support of the solution.

Amazon Web Services (AWS) (Sub-processor) - provide the Cloud hosting of Graphnet's and System C's internal support management software (Jira). If in order to resolve a particular incident the Customer needs to provide the Company with personal data, such as a patient's identifier, that information may be held temporarily in Jira before being deleted when the incident is resolved. No other personal or special category data will be held or available on Jira for any other purpose.

2.4.2 Principles and Accountability (Article 5)

Article 5 (2) and Article 24 require Data Controllers to demonstrate compliance, whilst implementing appropriate technical and organisational measures taking into account nature and scope of processing and the risks involved. This section outlines what is considered should be implemented to ensure measures are in place and compliance demonstrated.

(a) processed lawfully, fairly and in a transparent manner in relation to individuals;

[6] Article 29 Data Protection Working Party - Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679 April 2017

Lawfully

For processing to be lawful under Data Protection Legislation, justification, fairness and lawful basis needs to determined before personal data can be processed.[7] By case precedent 'fairness' encompasses the common law of duty.

In order for processing to be lawful necessity and proportionality need to be taken into account. In part this can be justified by the Care Act 2014 establishing the legal duty upon local authorities and health organisations to work together in order to provide integrated care.[8]

'Special category' includes health data. To comply with GDPR to process 'special category' data is prohibited unless at least one condition from Article 6 and one condition from Article 9 apply.

Article 6 and 9 – Legal Basis and Conditions for Processing

Article 6

- 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.

NB Public authorities will need to justify why processing is necessary to carry out their functions if using Art 6. (1) (e).

Article 9

- 9(2)(h) – Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, **medical diagnosis, the provision of health or social care or treatment or management of health or social care systems** and services on the basis of Union or Member State law or a contract with a health professional.

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)

As reinforced by:

[7] https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr/ Page 9

[8] http://www.legislation.gov.uk/ukpga/2014/23/section/3/enacted

DPA 2018 Schedule 1, Part 1 (2) – (1) condition is met if the processing is necessary for health and social care purposes…(2) means the purposes of (c) medical diagnosis, (d) provision of health care or treatment, (e) provision of social care and (f) management of health care systems or services or social care systems or services.

Recital 53 clarifies this processing as:-
Special categories of personal data which merit higher protection should be processed for **health-related purposes only where necessary to achieve those purposes for the benefit of natural persons** and society as a whole.

Fairly and Transparently

In order for the processing to be fair it must be expected by the Data Subject, this will be achieved by effective and robust communications through robust Fair Processing activities. Patients have the right to know how Data Controllers are processing their data so any proposed use is understood and expected. This is balanced with the duty to share information for the provision of Direct Care. Any action that fails to achieve fairness could potentially end up in a prosecution under Data Protection legislation. In order to achieve fairness the use(s) must be effectively communicated. There is no test of reasonableness as to how much effort must be made in this communication, however it is generally accepted that the more unexpected or sensitive the data, the more effort must be made in ensuring Data Subjects are aware. Therefore, in order to present the proposed use and other relevant information (expanded on in Appendix C) robust and effective Fair Processing is carried out through various channels of communications.

Article 14 outlines that if the data was not originally provided by the Data Subject they must be informed where the data has come from. By being clear and explicit the OHC partners will enable this requirement to be met.

Fair Processing materials will be developed in conjunction with and signed off by the OHC IG Steering Group to ensure all partners are involved in the decisions regarding messages, formats and methods. ICO Data Sharing Code of Practice outlines when there are multiple organisations best practice is to work together to ensure consistent messages are developed and issued.[9]

The 8th Caldicott principle - Inform patients and service users about how their confidential information is used – highlights how there should be no surprises and clear expectations to how confidential data is used and their choices.[10]

Right to Object

In order to object a citizen should discuss with their GP, if applicable this will then be recorded on the GP system with the relevant code. This code will then be used within OHC to ensure those individuals records will be restricted from view and access.

Patients whose data is recorded in OHC and are not registered with one of the participating practices, will be able to rais-pe their request by emailing OHC.Objection@nhs.net. They will need to provide full name, DOB and NHS Number for their request to be actioned centrally.

[9] https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf
[10] Eight_Caldicott_Principles_08.12.20.pdf (publishing.service.gov.uk)

Due to the varying functionality of healthcare provider software systems (outside of GP systems) the approach of restricting the data rather than fully stopping the processing means that a more reliable and consistent approach can be met.[11]

Personal Health Record is only available if a data subject chooses to download the NHS App. E-appointments can also be viewed through the NHS App but it will only relate to MPFT, UHNM or NSCT patients. Individuals who download the app will have access to electronic appointment correspondence. They will continue to receive paper correspondence unless they notify the aforementioned organisations.

Children

Article 12 (1) states 'The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means.' Recital 58 highlights that GDPR provides special merit to the protection of children and therefore 'where processing is addressed to a child, should be in such a clear and plain language that the child can easily understand'.

Appendix C goes into more detail regarding how the Fair Processing requirements are met.

Personal Health Record is not applicable for children at this time.

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes;

Purpose Limitation

This principle requires the Controller to specify the processing and its purpose and to be explicit and to therefore not deviate from this. It requires processing to be completed only with legitimate purposes.

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;

Data Minimisation

Data sets within partner systems will contain a variety of administrative and clinical data, not all of which would be justified as being necessary for the purpose of Direct Care. Some data sets will clearly be for purposes other than Direct Care – such as Secondary Use Services (SUS) and some social care data based on costs and funding, other data sets may not be as clear cut. Data Protection Legislation requires that only limited data is to be processed that is needed to achieve the purpose, therefore the purpose for using the data has to be clear to be able to judge what data sets are required in terms of proportionality, relevance and necessity.

Only codified data is extracted from the partner systems. Once the applicable data sets are identified from the partner systems there will be the ability to identify any required restrictions on certain data from being included. It will also be confirmed there is the technical ability to adhered to this from

[11] The revised approach is outlined within the OHC COVID-19 Response Paper – March 2020 v1.3

partner systems, e.g.to ensure that data, which is not required to meet the purpose, does not get pulled from the master system to OHC. Partners carry out testing to ensure this is adhered to.

Furthermore, exclusion lists have been developed where statute restricts the use of using and sharing (detailed in Appendix A). These lists highlight which data sets will not be included in OHC, predominately highly sensitive data sets. Exclusion codes will prevent this data being processed and consequently not being uploaded; exclusion codes prevent data on Exclusion Lists being processed at any point.

There will be no extraction from free text fields. Free text fields are inconsistent in etiquette and in overarching categories between partners. In sharing Third Party data may also be put at risk. There is also a risk that the data recorded may be out of date.

Viewing data is determined by clinical need. A strict access model governs access given on a need to know basis for direct care purposes. Appendix B expands on how this will look.

Agreed data sets are identified and signed off to meet the overarching purpose of OHC and justified as being proportionate and necessary to meet that purpose. The identification of the data sets by each data provider is essential to inform the technical workstream for data migration and as part of the Fair Processing campaign in order to accurately inform citizens of the specific data being processed (in order to also then comply with Article 5 1 (a)).

Personal Health Record data sets viewable to data subjects are outlined in Schedule 1. Data added by data subjects will not be available to view by clinicians.

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay

Accuracy

Each Partner will be responsible for their own data accuracy, completeness and quality. Each partner has processes in place to ensure that there are regular opportunities for records to be updated.

Personal Health Record - Data added by data subjects will not be available to view by clinicians.

Up to Date

Accuracy of the data will have a dependency on the regularity of the extract. Regular extracts provide improved accuracy and reliability as updates in the source systems will be captured. OHC data will be refreshed either near real time or at least every 24 hours – depending on the provider.

Predominately OHC will be Read Only (the accuracy of this data being reliant on the next data extract/update), however, in a future phase there will be a write function for the purpose of care plans.

There is an assumption that all partners have local processes in place to ensure their data is accurate and up to date in the source systems.

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes subject to

implementation of the appropriate technical and organisational measures required by the GDPR in order to safeguard the rights and freedoms of individuals;

Storage Limitation

Each Data Controller remains responsible for compliance with this principle within the management of their systems and implementation of retention and disposal schedules. Therefore when a record is out of its retention this will be managed by the source systems and then reflected in OHC at the next data extract.

Data will be retained in partner source systems for time periods as defined in the Records Management Code of Practice for Health and Social Care 2021. In summary these include (but are not inclusive as some care records have nonstandard retention periods):

- Adult general health and care records are retained for 8 years after the patient was last seen
- Children's' general health and care records are retained until their 25th or 26th birthday (if 17 at the time they were seen), depending on when they were last seen
- GP records are kept until 10 years after the death of a patient
- Mental health records are kept for 20 years after the patient has last been seen, or 8 years after the death of a patient

OHC will predominately be a read only system however there will be the ability to for care plans to be created and developed by multi agencies. Any clinical decisions made will be recorded in the relevant partner system, the result of which would then be reflected in OHC at the next data extract flow.

It should be ensured that information used at the point of Direct Care to inform a clinical decision can be identified and reproduced to legal admissible standards as evidence for medico-legal purposes.[12]

There is an assumption partners have local processes in place to ensure data is held no longer than is necessary through locally managed retention and disposal schedules. Therefore once records are disposed of in the source systems this is reflected at next extract, so there is no data deletion (or ability to make records inaccessible) from OHC directly.

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

The data processed as part of the OHC is special category (sensitive) data and therefore robust security measures must be in place. The ICO states that it is good practice for an organisation sharing information to ensure it will be protected by adequate security by the recipient organisations.[13]

Under Article 32 (1) of GDPR all partners must ensure they have implemented appropriate technical and organisational measures to ensure a level of security appropriate to the risk. For example:

- Encryption and pseudonymisation of personal data
- Ability to ensure confidentiality, integrity, availability and resilience of systems and services
- Ability to restore access and availability in a timely manner in the event of physical or technical incident

[12] http://www.thecabinetoffice.co.uk/page28.html

[13] https://ico.org.uk/media/for-organisations/documents/1068/data_sharing_code_of_practice.pdf Page 25

- Regular testing, assessing and evaluating the technical and organisational measures effectiveness

The level of security will be determined taking into account the risks (as outlined by Article 32 (2)):

- Accidental or unlawful destruction
- Loss
- Alteration
- Unauthorised disclosure or access

Data Upload

For data transfers from all partners a SFTP/SCP server to server scenario will be utilised. Digital transmission will be encrypted using appropriate standards based processes and strong (256 Bit) keys, for in transit or at-rest. Data will be transmitted to and from Microsoft Azure data centres over secure N3 links to the partner networks.

The technical solution meets HL7 interoperability and ISO27001 Information Security Management System standards. OHC will only be available through an N3 connection, either integrated within the core system (Single Sign On) or through web interface with username and password. The suppliers shall provide the deliverables in accordance with Cyber-Essentials+ across the stack as well as at network level and the process, people and technology standards from the 10 Data and Cyber Security Standards.

Prior to live data being processed dummy, test data uploads is conducted which reviews the security measures being utilised.

Access

Access control is established to ensure only the right individuals have access to the data, taking into account the following controls.

Access to the OHC data for individuals within the direct care team will be through a restricted role based access model (RBAC). Further information can be found in Appendix B.

NHS App will be the interface for service users to access the Personal Health Record (PHR) and e-appointments letters.

Access provision is dependant on the method of access. If a partner accesses the system through Single Sign On (SSO) access will be determined and managed through the partners local starters and leavers processes and policy. If SSO is not being utilised access will be through by the partner organisations Service Desk and allocated Systems Admin. Therefore partners where SSO is not utilised will need to ensure local processes are implemented. Normal Starters/Leavers process within each relevant organisation should be utilised. It will be for each organisation to ensure that current users access authorisation processes will be validated locally before any request for access is processed.

Users will only see patients they have a legitimate relationship with. A user can only see a citizen record relating to their organisation – so for example if a citizen has no social care record/interaction

then the local authorities would not have access to those citizens OHC record and a GP practice would only have access to the OHC records of the patients linked to that practice.

The system has useable audit trail facilities to ensure access to records can be identified, either through the citizen record or access made by a specific user of the system. The audit facilities provide information regarding date and time of access and exactly what part of the OHC record was accessed. Access therefore can be monitored and audited when required, with each partner organisation having training available to them regarding how to process these requests. The Systems Admin role will have the authority and access to this functionality within the system. It is up to each organisation to appropriately allocate that role to relevant individual/s. In order to comply with GDPR Article 15 and the NHS Constitution this should also deliver the ability for citizens to be provided with information as to who might have accessed their information.[14] There are deemed three key scenarios where audit reports may be required:

- **Spot checks**: As part of assurance work quarterly random spot checks will be conducted on the access audit reports to assess whether appropriate access is being satisfied. This will require each partner organisation to produce an access report sample of 25 service users randomly selected on a quarterly basis. The access reports will be reviewed by identified Information Governance leads of each organisation. Findings will be reported back to the IG group as an assurance group, for example a summary of findings and if any action was taken. Internal processes within each organisations would then take responsibility for any misconduct. Internal processes would be expected to be completed within two weeks of the report being run. This is a standing agenda item for the OHC IG group.

- **Investigations** – Partner organisations named IG lead should request from their local Systems Admin relevant access logs/audit trails when required for investigations. It should be expected that the information would be provided within 72 hours. Only named IG leads should be requesting this information and consequently being responded to by Systems Admin. Internal processes of the requesting organisation would then apply for investigating. Each organisation are required to report back to OHC IG group regarding volumes and specific issues that may need considering wider.

- **Data Subject Requests** – Partner organisations named IG lead should request from their Systems Admin relevant access logs/audit trails when required for information requests by Data Subjects. These requests should be responded to within 72 hours and to the nominated/named IG lead. Each organisation will report figures back to the OHC IGSG. NB this will require consideration and updating when OHC evolves to be the primary source system (e.g. when care plans are being utilised).

Governance

Each partner organisation will have appropriate technical and organisational measures in place to comply with Article 5 (f). The Information Sharing Agreement outlines agreed standards ensuring each partner will take reasonable steps towards appropriate technical and organisational security measures. This requirement will also be somewhat illustrated by each partner organisation being

[14] Respect, Consent and Confidentiality, NHS Constitution - https://www.gov.uk/government/publications/the-nhs-constitution-for-england/the-nhs-constitution-for-england

compliant with NHS Digital Data Security and Protection Toolkit (DSP Toolkit). This satisfactory compliance requirement is outlined within the Information Sharing Agreement.

A legally binding contract is in place with the supplier and includes standard contract clauses and assurances regarding security in order for this principle to be complied with. IG leads of the partner organisations should be involved and provided the opportunity to review the relevant section of the contract for their locality.

Incidents
The Information Sharing Agreement outlines partner responsibilities if a breach occurs, in summary that each will follow incident reporting procedures as required by Data Protection Legislation. Contact details for relevant IG roles within each partner organisation feature within the ISA. The OHC IG Steering Group will ensure incidents can be monitored when applicable and lessons learned be benefited from. For incidents clearly originating from one organisation these will be dealt with by that organisation through their normal incident processes. For incidents where the source is not clear or whereby two or more organisations are involved a coordinated review and response of the incident will be conducted with IG representatives from each organisation through an urgent held IG group meeting (whether in person or virtually). A 24 hour deadline from realising should be instilled for informing each organisation and a 48 hour deadline for the group to meet to ensure the 72 hour deadline for reporting to the ICO is met if deemed required. IG contacts and contact details, including Data Protection Officers (DPOs), are outlined within the Information Sharing Agreement appendices. NB this section will require updating for Care Plans as they will be jointly created records which will have implications regarding data controller and owner of the information.

Availability
Data within OHC is duplicate; in the event of a failure recovery procedure will revert back and extract a copy of the source data. In case of non availability of the system source systems and previous methods of information sharing will entail (for example email, fax, telephone). NB this will change when Care Plans are utilised as they will be created in OHC and therefore the single source of that information.

Backups are held offsite (in UK)[15] and the disaster recovery systems achieve Recovery Point Objective (RPO) of 1 hour and Recovery Time Objective (RTO) in 4 hours. These are regularly tested.[16] The supplier manages disaster recovery and business continuity arrangements, including developing the DR for the system. Annual testing of both occur.[17] Backups are stored for 30 days, which is the default Microsoft retention policy. They will be stored within the Azure Blob Storage which is encrypted at rest.

https://docs.microsoft.com/en-us/sql/relational-databases/backup-restore/sql-server-backup-and-restore-with-microsoft-azure-blob-storage-service?view=sql-server-ver15

The contract with supplier outlines the standard committed service level is in line with industry standard and apply to the hosted environment (availability of 99.50% and priority one incident resolution within 4 hours).

[15] Overarching contract Appendix 2 to Annex 7 – 4.4.3 - Security Statements, Page 63.
[16] Overarching contract Appendix 2 to Annex 7 – 3 - Security Statements, Page 63.
[17] Overarching contract Annex 5 - Information Security Management Plan, Page 50.

Training
Each partner organisation is required to have all staff trained in appropriate data protection training as is a mandatory requirement outlined by the DSP Toolkit and is outlined in the Information Sharing Agreement (Section 4).

The Processor commits its staff have undergone adequate training in the use, care, protection and handling of personal data.[18]

Processor
Under Data Protection Legislation processors are subject to liability for failure to comply with their contractual obligations to their controllers and are open to direct action by regulators. Under the legislation it must be ensured that there is a contract evidenced in writing, outlining that the processor must only act under instruction of the controllers. The contract must also have a level of security which is imposed by Article 32.

As outlined in section 2.4.2 the Data Processor is the System C and Graphnet Care Alliance who are the providers of the CareCentric system. The system will be hosted by Microsoft Azure Cloud Computing Platform and Services, as subcontracted by System C and Graphnet Care Alliance. Within the contract it is outlined that the Data Processor will not sub contract without written authorisation and assessment by the Data Controllers. Also outlined with the contract is that the supplier will be required to provide assurance in regards to compliance with the Data Security and Protection Toolkit and ISO270001 (to which they are certified). No data will be processed until partners are confident in the data protection elements of the contract being fit for purpose.

Confidentiality and Integrity (Security)
The contract confirms the supplier undergoes external penetration testing and are ISO9001 and 27001 accredited and independently audited. Any weaknesses or vulnerabilities identified will be actioned within appropriate timescales, particularly those identified as high risk. Graphnet are obligated to adhere to all standards required and will be in breach of contract should the standards not be met.

The data will be hosted by Microsoft Azure Cloud Computing Platform and Services. Servers are held in the UK. The data is processed in accordance with the fourteen National Cyber Security Centre cloud service security principles.[19]

The contract held with the supplier will suitably cover maintenance, outlining what is expected of them in terms of maintaining data availability and integrity.

Personal Health Record
The NHS App[20] will be utilised for individuals to log into Personal Health Record. Owned and run by the NHS the app can be downloaded by an individual and required to set up an NHS login. NHS login requires an individual to prove who they are by using driving licence, passport or European national

[18] Overarching contract Annex 7 – Processing of Personal Data, Page 54.
[19] Overarching contract Annex 7 – Processing of Personal Data, Page 62.
[20] https://www.nhs.uk/using-the-nhs/nhs-services/the-nhs-app/

identity card.[21] Data is sourced and stored within CareCentric. Access would then be through username and password. Application uses end to end encryption.

Article 5(2) requires that 'the controller shall be responsible for, and be able to demonstrate, compliance with the principles.'

Accountability

The partner organisations and any 3rd Parties should display a culture of privacy, which includes the relevant organisational and technical measures in order to implement the principles. To comply with this processing activities should be documented.

Under Data Protection Legislation it is mandatory for public authorities, and organisations processing special category data on a large scale, to have a Data Protection Officer (DPO) in place. Large scale considerations include the number of Data Subjects involved, the volume of data and duration of the processing activity. The supplier has a DPO in place.

This accountability requirement is reinforced by the NHS DSP Toolkit as it requires organisations to develop and manage an Information Asset Register, the output of which goes some way to meet Article 5 (2).

It is assumed each organisation has a suitable governance structure which meets Data Protection Legislation requirements.

Article 30 – Recording of processing activities

As per Data Protection legislation each partner organisation processing data will be registered with the Information Commissioners Office (ICO), thereby specifying and being explicit about the processing of personal data.
Article 30 requires Data Controllers to maintain record keeping and records of processing activities, which would then be reflected within Fair Processing. The ROPA for OHC features within the ISA.
Recital 82 states 'Each controller and processor should be obliged to cooperate with the supervisory authority and make those records, on request, available to it, so that it might serve for monitoring those processing operations'.

2.4.3 Rights of the Data Subjects (Article 12 – 22)

Article 12 – Exercising the Rights of the Data Subject	

Article 12 outlines how communications in relation to data subject rights should be exercised:

- Concise, transparent, intelligible and easily accessible form, using clear and plain language
- Information can be provided orally (dependant on suitable verified ID of the requester)
- Requests must be actioned without undue delay and in any event within a month (30 days) of receipt
- The requester must be provided information in regards to how to lodge a complaint with the ICO should they wish to
- No fee should be sought for actioning any requests (unless they are found to be manifestly unfounded or excessive)

[21] https://www.nhs.uk/using-the-nhs/nhs-services/nhs-login/

OHC Core Read Only Record
Requests relating to a Data Subjects data are referred back to the source provider of the data, therefore each Data Controller will be required to respond to Data Subject rights relating to their own data. A local process must be in place to ensure partners frontline staff are aware of the procedures relating to Data Subjects exercising their rights.

Personal Health Record
When information is added to the PHR by a service user it becomes part of their record within One Health and Care, however would not be presented to users of the system. If a data subject deletes a value this would then be replaced with new value (which could be a blank field). There is nothing to indicate that a value has been deleted other than looking in the audit trail in the database.

Article 15 - Access

Under Data Protection Legislation, Data Subjects have the right to request confirmation if data is being processed about them and a copy of that information from the Data Controller. As well as a copy of the data the following information should be provided:

- Purpose of the processing
- Categories of the information and the recipients
- Retention of the data
- The rights that the Data Subject has in relation to the data
- Right to lodge a complaint with the ICO
- The source of the data
- And whether any automated decision were made, the logic and consequences if applicable.

OHC Core Read Only Record
A shared care record can complicate matters in that it may not initially be clear who the overarching Data Controller is however OHC shows which source the data is from and is referred to as 'tenancy'. This must be considered within local process guidance to ensure effective steps are in place.

Personal Health Record
Schedule 1 outlines the different information aspects and data flows that are involved.

Article 16 - Rectification

A Data Subject has the right to request incorrect or incomplete information held about them is rectified. This is particularly relevant when an individual for example provides their consent to processing as a child and then later wishes to remove any relevant data.

OHC Core Read Only Record
Requests dealt with by the source provider.

Personal Health Record
Rectification of data added by the data subject through Personal Health Record can be managed by the data subject themselves. Other requests would be dealt with by source provider.

Article 17 - Erasure

Data Subjects have the right to request their personal data is erased (the right to be forgotten). There are certain grounds that must apply for this request to be processed by a Data Controller.

The right to erasure of data without undue delay applies if the following is applicable:

- Data is no longer necessary
- The Data Subject has withdrawn their consent and there is no further legal grounds to process the data (not applicable as ICR not consent based)
- Successful objection under Article 21 (Right to object)
- Data is being unlawfully processed
- There is a legal obligation to erase
- The data is being processed online with parental consent and the child has reached competency to withdrawn their own consent (not applicable as ICR not consent based)

If the above points apply then this right can be exempt from being put into action if the processing:

- is based on freedom of expression
- is based on a legal obligation
- is due to public health in the public interest
- purpose is archiving, scientific, historical or research which would be damaged if removed
- is due to establishing, exercising or defending legal claims.

OHC Core Read Only Record

This is therefore not an absolute right, it is to be evaluated on a case by case basis by each applicable data controller.

Personal Health Record

Data added by a data subject through signing up to PHR access that data then forms part of their clinical record, however is not viewable by system users. If a data subject deletes a value they have added this would then be replaced with new value (which could be a blank field). Data subjects will be clearly and transparently informed data added will be included within the Business Intelligence function of OHC.

Article 18 - Restrict processing

A Data Subject can request that their personal data is restricted from being processed, if one of the following applies:

- The accuracy of the data is contested and is being looked into
- It has been found the processing is unlawful
- The data needs to be kept for the Data Subject to process a legal claim
- The Data Subject has objected to the data being processed so it has been 'quarantined' and therefore access is physically prevented

If this right is actioned the data can then only be used if:

- Data Subject provides consent
- The overarching organisation are required to use the data to action a legal claim
- The data is needed to protect another individual for example from harm

OHC Core Read Only Record

There will need to be a mechanism for restricting processing if a legitimate request is put forward.

Personal Health Record

There will need to be a mechanism for restricting processing if a legitimate request is put forward.

Article 20 - Data portability

Data Subjects have the right to request data in a structured, commonly used, machine readable format and for it to be transferred to another provider if required. For this right to be actioned the processing must be: ➢ Either based on consent from the Data Subject or as part of a contract between the Data Controller and the Data Subject; and ➢ When the processing has been carried out by automated means. Therefore this right is not applicable in relation to OHC (see legal basis Section 2.4.2).
Article 21 - To object
Data Subjects have the right to object to their data being processed. For this to be actioned the impact on the Data Subject must override the need for us to process the data, for example there must be compelling legitimate grounds to continue to process the data. This may be legal or statutory reasons for example. GP practices will manage objections centrally through their source systems, if applicable the data will then be restricted, so unable to view or access by any user of the system. Updates will be picked up and updated at each data extraction. NB The above highlights the process under the purpose of direct care, this section requires considering to reflect secondary use requirements when this phase is being initiated.
Article 22 - Automated decision making and profiling
There will be no automated decision making involved in OHC regarding the Data Subject.

2.4.4 Transfers to Third Countries (Article 44/45)

Article 44/45 – Transfers to Third Countries	
Bound in contract that data will not be transferred outside of the UK or EEA. The supplier is based within the UK (including their server and technical support provision). The specification stated as a requirement that the supplier will be UK based.	

3. Data Flows

3.1 Data Flow Diagram

At a high level the data flow will work as below:

Direct link with Data Controller: the ICR has a direct link to each DC in order for data to be extracted. Any involved partner would then able to view the output.	DC A (Acute Trust) Interface → ↔ DC Viewing DC B (Social Care) Interface → ICR ↔ DC Viewing DC C (GP System) Interface → ↔ DC Viewing

3.2 Summary Data Flows

3.2.1 Near real time

Organisation	Type of Services Provided	System Name
University Hospitals of Derby & Burton NHS Foundation Trust (UHDB)	Emergency and Acute Hospital Services	**Meditech** **Medisec**
University Hospitals North Midlands NHS Trust (UHNM)	Emergency and Acute Hospital Services	**Medway EPR –** EPR solution providing a single MPI/PAS and reporting solution and will provide data feeds to OHC. **iPortal –** portal primarily draws together key clinical information within UHNM to provide clinicians with an overview of activity, diagnostic results, letters and notes. **GraphNet Carecentric –** provides a cross-organisational portal that is capable of drawing together data from disparate systems.
The Shrewsbury and Telford Hospital NHS Trust	Emergency and Acute Hospital Services	**Medway EPR /Sema Helix PAS –** EPR solution providing a single MPI/PAS and reporting solution and will provide data feeds to the OHC
The Robert Jones and Agnes Hunt Orthopaedic Hospital	Emergency and Acute Hospital Services	**Lorenzo –** EPR solution providing a single MPI/PAS and reporting solution and will provide data feeds to the OHC**.**

		GraphNet – provides a cross-organisational portal that is capable of drawing together data from disparate systems.
The Royal Wolverhampton NHS Trust	Emergency and Acute Hospital Services	**Silver link / inhouse system**
Walsall Healthcare NHS Trust	Emergency and Acute Hospital Services	**DXC/Orion**
The Dudley Group NHS Foundation Trust	Emergency and Acute Hospital Services	**All Scripts**
Sandwell and West Birmingham Hospitals NHS Trust	Emergency and Acute Hospital Services	**Cerner**

3.2.2 least every 24 hours

Organisation	Type of Services Provided	System Name
Staffordshire and Stoke-on-Trent GP Practices	Primary care provision	**EMIS –** clinical system widely in use amongst the LHE's GP practices. **Docman -** GP document management system with an existing high penetration in Primary Care. NB *All but 11 practices across Staffordshire and Stoke on Trent utilise the EMIS clinical system. The remaining practices utilise TPP System One, Microtest or INPS Vision.*
Shropshire, Telford and Wrekin GP Practices	Primary care provision	**EMIS –** clinical system widely in use amongst the LHE's GP practices. **Vision** - clinical system widely in use amongst the LHE's GP practices. **Docman -** GP document management system with an existing high penetration in Primary Care.

Black Country and West Bimingham GP Practices	Primary care provision	**EMIS –** clinical system widely in use amongst the LHE's GP practices. **Vision** - clinical system widely in use amongst the LHE's GP practices. **Docman -** GP document management system with an existing high penetration in Primary Care.
North Staffordshire Combined Healthcare NHS Trust (NSCHT)	Provider of Adult and Older Peoples mental health services; learning disability and primary care services	**Lorenzo** – the EPR solution.
Midlands Partnership Foundation Trust (MPFT)	Provider of Community Services Provider of Adult and Older Peoples mental health services; learning disability and primary care services	**Rio** – the EPR solution
Shropshire Community Health NHS Trust	Provider of Community Services	Rio – the EPR Solution.
Birmingham Community Healthcare NHS Foundation Trust	Provider of Community Services	**RiO**
Black Country Healthcare NHS Foundation Trust	Provider of Community Services	**RiO**
Dudley Integrated Health and Care NHS Trust	Provider of Community Services	**RiO**
Staffordshire County Council (SCC)	Social Care Provision	**Care Director** – social care system.
Stoke-on-Trent City Council (SOTCC)	Social Care Provision	**Liquidlogic** - social care system.
Shropshire Council	Social Care Provision	**Liquidlogic –** social care system.

Telford and Wrekin Council	Social Care Provision	**Liquidlogic** - social care system.
City of Wolverhampton Council	Social Care Provision	**OLM**
Dudley Metropolitan Borough Council	Social Care Provision	**Liquidlogic - social care system.**
Sandwell Metropolitan Borough Council	Social Care Provision	**Liquidlogic - social care system.**
Walsall Metropolitan Borough Council	Social Care Provision	**Mosaic**

3.2.3 Data Viewers

Organisation	Type of Services Provided	System Name
West Midlands Ambulance Service NHS Foundation Trust (WMAS)	Emergency and Non-Urgent Patient Transport	**Cleric**
Continuing Health Care Service NHS Midlands and Lancashire CSU	Continuing Health Care	**Adam**
Vocare Ltd	Out of Hours/Urgent Care GP Services and NHS 111	**Adastra**
Shropshire Doctors Limited (Shropdoc)	Out of Hours GP Services and NHS 111	

Schedule 1 – Personal Health Record

1. Introduction

The Personal Health Record provides a service user with access to their health and care records in a single solution accessible on the web or via dedicated iOS and Android apps optimised for both mobile and tablet form. It aims to improve patient engagement and allows individuals to be better informed and empowered with information about their health and care at their hand.

Individuals gain access to their Personal Health Record if they chose to download the NHS App – summary data held within One Health and Care will then be presented through their device.

2. Access and Fair Processing

The Privacy Notice and use of Personal Health Record is based upon direct care. The registration on informed consent – informing user that email address will be used to validate their account, authenticate and match to their health record. Therefore allowing the individual to log in to their account and own a copy of a summary health information about them. This process is therefore assessed to be a legitimate use of the data and in line with the overarching purposes of One Health and Care.

The collection, storage and display of user-entered health information is a key element of the Personal Health Record model and provides the user with an opportunity to be actively involved in the information about their health. Since this process is led by the data subject themselves, the legitimacy of the data entered is also determined by the data subject. A Personal Health Record Privacy Notice sits along side the OHC Privacy Notice, and will reflect the 'User-managed personal information' aspect and outline the types of information that might be involved, and therefore supports the direct care purposes of OHC system as a whole. This information will be provided at point of downloading the app.

Personal Health Record **service is not a real-time messaging and alerting system, health and social care professionals will not have access to the data provided by service users/patients.**

Access provision to **a non-professional carer,** for example a family member, is solely managed by the service user. The functionality for access to be provided to an individual as the service user is incapable of providing consent for access is not yet available.

3. Key features

- Real time integration between the myCareCentric and CareCentric's Integrated Digital Care Record and third-party solutions with real-time interfaces
- Secure login across different device platforms
- Optimised views for different platforms and form factors
- Sign posting to trusted information is available - which can be tailored to specific needs or as the patient's activation measure changes
- Personal Passport feature allows the citizen to record information about themselves that they wish to make a note regarding important factors they wish to discuss
- Lifestyle factors can be recorded so that personalised goals and actions can be set accordingly

- Landing Pages configured to meet the patient cohort
- Configurable and localized branding
- Specific users group view
- Access to appointments and letters (cannot amend currently)

4. User Sourced Information

Personal Health Record will pull information from the Integrated Care Record One Health and Care; providing a summary view of an individuals record. Data subjects will be able to maintain a health diary and self-record information such as blood pressure, blood sugar, weight, personal goals and over the counter medication and the ability to link up information from fitness wearables such as Fitbit, Apple and Garmin.

Any information added to the app will then be available for data analysis under secondary use purposes, but not directly available for healthcare teams to view. It will only be used for secondary use purposes once a separate DPIA has been completed and approved. This will be made clear to service users and healthcare teams so they are fully informed of the system functionality and limitations.

The categories of data used in Personal Health Record registration process are:

- Email address;
- Mobile number;
- First name; and
- Surname.

5. PHR Fields

In addition to data provided during the registration process the categories of Personal Health Record data that can be added and managed is as follows.

Feature	Content and Feed
PHR View: Home	
Future Hospital Appointments	Currently just Acute hospital activity (outpatients, inpatients and A&E) For information screen for service user.
It's OK to Ask	Service user recorded information – allows them to write notes in preparation for their next appointment. Will not be stored within CareCentric. 'Make a note of any questions you would like to ask your healthcare team on your next visit'.
Self-Recorded Measurements*	Patient recorded information A service user may delete a value if it has been entered and saved incorrectly. The individual cannot edit the value once it has been saved (it can only be deleted and re-entered). AI/BI is not involved initially however future phases may flag for example if a threshold is met when self recorded data is added. In order to future

	proof it will need to be made clear in the comms and FAQs that data added by the user will go into the BI tool.
Goals*	Patient recorded information. Personal Health Record will not be used to post information regarding local initiatives to help meet those goals. Language in regards to the comms and FAQs needs to be considered, for example 'Goal based care planning' is a term used by mental health so would have different connotations to the goals within the Personal Health Record.
All About Me*	Patient recorded information. For example this could be who to contact in an emergency. If a service adds information that differs to that that is held within the ICR there would be no data quality issue as the information is in separate section / tile within the solution.
Garmin wearables module*	Patient recorded information. Any information proactively uploaded from a device may also then be used for secondary use purposes. A user would have to actively connect their device to the app and accept that the data would be transferred. This data would then be viewable to the user through Personal Health Record and stored within myCareCentric. In order to erase the data the user would have to write over the data previously uploaded. The data would not be viewable to OHC users however it would then be included within the BI functionality. The wearable must be paired with the app in order for the data to be shared – this would be through a positive action by the individual. Comms and FAQs highlight this. In terms of amending wearable data it comes directly from the device that has been linked to the PHR (rather than the person entering the data). If the data can be changed on the device, then the associated updates will be seen in the PHR.
Fitbit wearables module*	Patient recorded information. As Garmin above
Link to NHS e-Referral Service	Link to external website
Link to NHS Service Search	Link to external website
Link to NHS Live Well website	Link to external website
Contact Us	OHC email address.
FAQs	Section requires review/update Updated and provided on OHC and partner websites.
Feedback	Link to SurveyMonkey Questionnaire

	Anonymous questionnaire regarding the app.
Licences and Attributes	Licences and Attribute data listed
Privacy Policy	Section requires review/update Will link to Staffordshire & Stoke on Trent wide Privacy Policy. Relevant URL will need to be provided. Policy will also include a Cookie Policy.
PHR View: Medication	
Recent Medication View All Medication - Repeats - Previous - Over the Counter	GP prescribed medication, including repeat prescription and recent GP provided vaccinations. Self recorded medication can be added within the 'Over the Counter' section (not viewable by system users). Once entered you cannot erase this information however the user can mark as 'I am No Longer Taking This Medication'. Shows only GP prescribed medication.
Link to NHS Medicines A-Z	Link to external website
Recent Vaccinations View All Vaccinations	GP vaccinations only There is only the facility in the system to report on GP administered vaccinations, not community (for example, MPFT). This will need to be made clear in the comms / FAQs for users to ensure there is this understanding.
PHR View: Appointments & Letters	
Next Appointment Past Appointments Hospital Admissions A&E Attendances	Data within section used for e-appointments aspect. Currently just Acute hospital activity (outpatients, inpatients and A&E). Future and past appointments together with A&E Attendances and hospital admissions. UHNM, MPFT and NSCT are working to enable electronic appointment letters.
Letters	Letters associated to the patient.
PHR View: My Health	
Results - Recent - View All ▪ GP ▪ Hospital	GP test results, known allergies, family history, medical problems, lifestyle and measurements such as blood pressure. **GP results -** There will be a dependency on what/when the GP results are sent via the GP extracts. This would also apply to any results from other settings. GP results are only sent to the Shared Record (and therefore available via Personal Health Record) once they have been marked as "filed" in the GP system so someone has seen and acted upon them where appropriate. **Hospital results** (future feed) - It is common with other results to have a 2-3 day delay before them being sent to CareCentric. A delay will be built into the system so they do not immediately show (until the clinician has viewed and checked).

	***Training dependency in that clinicians will need to know timing of when results will show in Personal Health Record and what will trigger the results showing.**
View Medical Problems - Active - Past - Link to the NHS A-Z	GP problems Diagnosed problems such as Diabetes.
View / Add Allergies - From GP - Self-Recorded	GP Allergies plus anything that has been recorded by the patient. User can remove or amend data they have entered.
View Family History	GP Family History Items that has been recorded as a family history i.e. Glaucoma, Diabetes etc…
View Lifestyle	GP Lifestyle Information relating to Smoking and Alcohol, Exercise and Diet.
View GP Measurements - Blood Pressure - Height, Weight and BMI	GP Vitals Data from GP system.
Link to Lab Test on-line UK website	Link to external website
Link to NHS Live Well website	Link to external website

6. E-appointments

Personal Health Record will also be used to view appointment correspondence to applicable patients at UHNM; MPFT and NSCT– this is referred to as e-appointments. Those who wish to can continue to receive paper letters. The latter being provided by Synertec – a separate DPIA has been conducted by UHNM covering this activity. The e-form for e-appointments is provided by Graphnet. The preferences in relation to e-appointments and letters is held within the clinical system at the participating organisations – MPFT, UHNM and NSCT. For the pilot group there will 3 months worth of letters uploaded into the solution in March 2021.

Individuals that are not registered at a Staffordshire or Stoke-on-Trent GP practice will receive a notification that they have an appointment letter via the NHSApp and then the individual will be navigated to the web version.

7. Future considerations

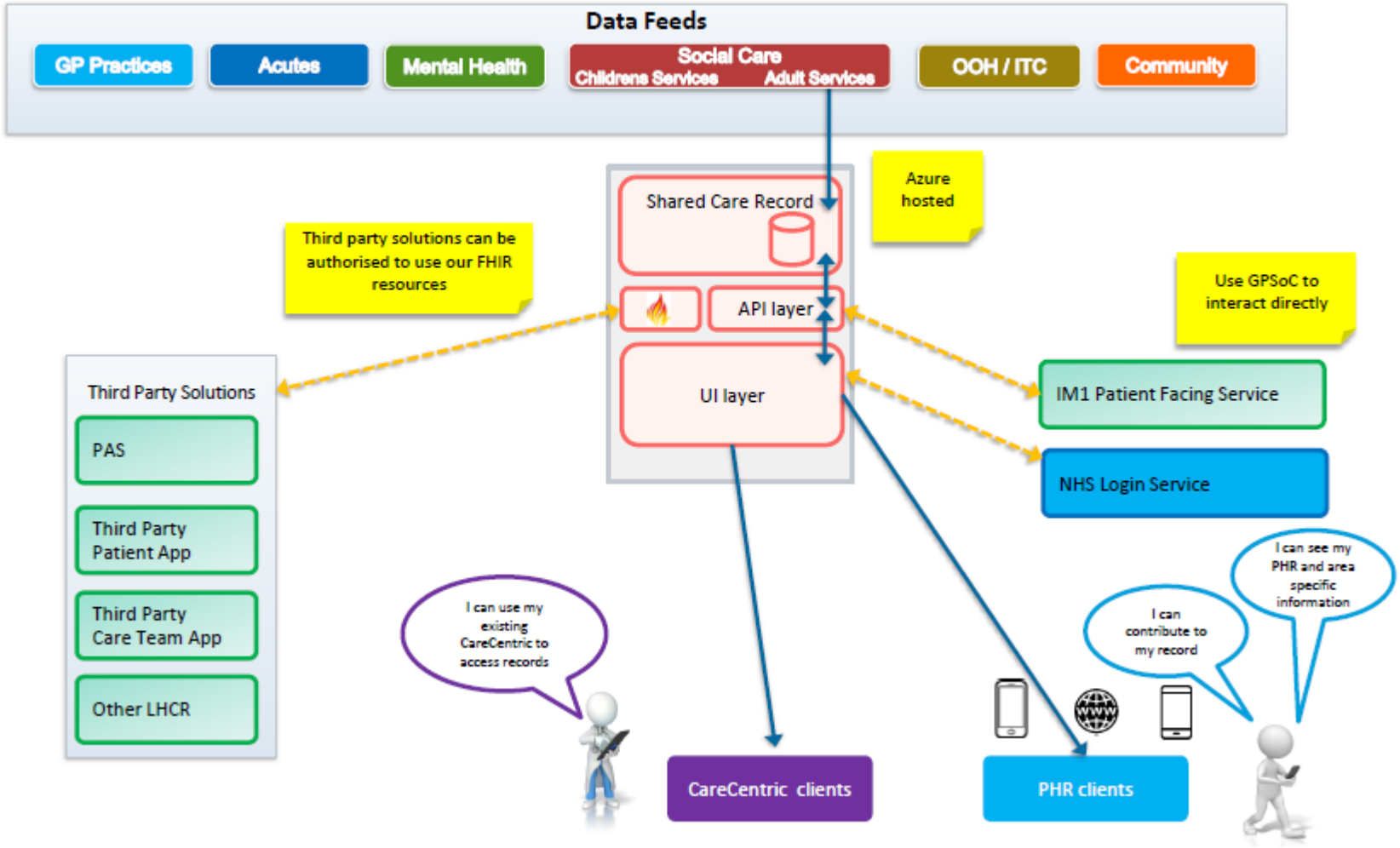
- Appointments (manually entered in an organiser view)
- Cancer Care symptoms (so the Oncology team can track progress)
- Weight/Blood pressure/Blood sugar
- Activity/Alcohol intake/smoking
- Care Plan
- RESPECT documentation
- Prescreening questionnaire
- Consent for treatment

8. PHR Data Flow

A	B	C	D	E	F	G
From who	**To who**	**What?**	**Why?**	**When? (Frequency)**	**How? (Transfer and storage -security and access)**	**Retention period**
CareCentric Shared Record	myCareCentric PHR	Health & Social Care data e.g demographics, appointments, letters, blood results	To enable patients to access information relevant to the management of their health & wellbeing	On access to the patient record or upon refresh of specific hubs within the app	Transfer via 256-bit TLS https. Stored encrypted at rest with AES 256bit.	Dependent upon the patient retaining their PHR access. All data is synced in the main Carecentric data store where local retention policies apply.
Citizen	myCareCentric PHR	Particular patient events and information as consented by the individual. Data may originate from connected medical devices and fitness apps	Contributes to the overall picture of an individuals health and wellbeing. Can be shared with the Care teams at the patients consent. Can assist the patients own management of their health & wellbeing	Variable	Transfer via 256-bit TLS https. Stored encrypted at rest with AES 256bit.	Dependent upon the patient retaining their PHR access. All data can be synced in the main Carecentric data store where local retention policies apply (upon patient consent).
myCareCentric PHR	CareCentric Shared Record	Particular patient events and information as consented by the individual. Data may originate from connected medical devices and fitness apps	Contributes to the overall picture of an individuals health and wellbeing. Can be shared with the Care teams at the patients consent. Can assist the patients own management of their health & wellbeing	Variable	Transfer via 256-bit TLS https. Stored encrypted at rest with AES 256bit.	Dependent upon the patient retaining their PHR access. All data can be synced in the main Carecentric data store where local retention policies apply (upon patient consent).

Standard Network Topology for PHR

Graphnet Integrating Care



Appendix A - Data Exclusions

Legal restricted data will be excluded from the Integrated Care Record, meaning they will never leave their originating systems. The below outlines the data exclusions which are defined as 'sensitive' by law and required to be refrained from being included within OHC.

Legally Restricted Data	
IVF, fertility treatment and embryology	Human Fertilisation Act 1990 as amended by the Human Fertilisation and Embryology (Disclosure of Information) Act 2004
HIV / AIDS	AIDS (Control) Act 1987
Venereal disease and Sexually Transmitted Diseases (STI)	NHS (Venereal Diseases) Regulations 1974; NHS Act 1977, NHS Trusts and Primary Care Trusts (Sexually Transmitted Diseases) Directions 2000
Gender realignment	Gender Recognition Act 2004[22]
Adoption	Adoption and Children Act 2002

Data that individuals would not expect to be routinely disclosed	
Termination of pregnancy	Sensitive data.
Specific information collected during an enquiry into safeguarding concerns	Sensitive data arguably not relevant to provision of care.
Carer records	This refers specifically to personal data regarding a carer (outside the definition of a professionally employed carer) which would be defined as Third Party data. For example a family member or friend of the subject.
Service user financial status and assessment	Data arguably not relevant to provision of care.
Complaints	Could be perceived to prejudice care.
Convictions and imprisonment	Specific detail would be defined as sensitive data and is not relevant to provision of care.
Abuse (physical, psychological or sexual, by others)	Sensitive data. NB A 'flag' however will be presented to inform users more information needs to be sought from source if required.

This list is not exclusive and can be reviewed and amended as required.

[22] It is an offence to disclose protected information such as a person's gender history after that person has changed gender.

Appendix B – Access Model

#	RA Job Role* (Registration Authorities and Smartcards)	RA Job Role Code	Alternative RA Code	CareCentric User Group / RBAC Role	Functionality Permissions Level**	Landing Page Used*** (Patient Data Access)	Notes/ Description
1	Admin/Clinical Support Access Role	R8008		Admin/Clinical Support	Level 1	Admin Clinical Support	
2	Clerical Access Role	R8010		Clerical	Level 1	Admin Clinical Support	
3	Receptionist Access Role	R8009		Receptionist	Level 1	Admin Clinical Support	
4	Clinical Practitioner Access Role	R8000		Clinical Practitioner	Level 2	Common	
5	Community Mental Health Nurse	R1975 (w)	R8001	Community Mental Health Nurse	Level 2	Social/ Community/ MH	
6	Community Nurse	R0700 (w)	R8001	Community Nurse	Level 2	Social/ Community/ MH	
7	Unscheduled Care	Unmatched		Unscheduled Care	Level 2	Unscheduled Care	Added as need to show data in different order to unscheduled/ emergency care professionals
8	General Medical Practitioner	R0260 (w)	R8000	General Practitioner	Level 2	General Practitioner	Needed to show data in different order for GPs
9	GP Practice Manager	Unmatched		GP Practice Manager	Level 2	General Practitioner	
10	Health Professional Access Role	R8003		Health Professional (Allied)	Level 2	Common	From RA: "A generic Health Professional role to cover all allied and other health professionals working in primary, secondary care, community care and mental health."
11	Medical Secretary Access Role	R8006		Medical Secretary	Level 2	Common	Medical Secretary that has access to Common Landing Page. If less than full data access required, select one of the Admin Clinical Support roles
12	Midwife Access Role	R8016		Midwife	Level 2	Common	
13	Nurse Access Role	R8001		Nurse	Level 2	Common	
14	Paramedic	R1070 (w)	R8003	Paramedic	Level 2	Unscheduled Care	
15	Pharmacist	R1290 (w)	R8003	Pharmacist	Level 2	Common	
16	Psychiatrist	R1981 (w)	R8000	Psychiatrist	Level 2	Social/ Community/ MH	
17	Senior social worker (adults)	R9570		Social Care	Level 2	Social/ Community/ MH	Added October 2017, as distinct from Social Worker
18	Social Worker Access Role	R8014		Social Worker	Level 2	Social/ Community/ MH	
19	Healthcare Student Access Role	R8004			TBC	TBC	From RA: "A generic Healthcare Student role to cover all staff currently undertaking training working in primary, secondary and community care, who require access to view detailed health records."
20	Other	N/A			TBC	TBC	A catch-all for any other roles
21	Audit Manager	R5100 (w)	R8001	Audit Manager	Level 3	Common	Role recently added
22	Caldicott Guardian	R5105		Caldicott Guardian	Level 3	Common	
23	Privacy Officer	R0001		Privacy Officer	Level 3	Common	
24	Systems Support Access Role	R8015		Systems Support	Level 4	Common	System and User Administration (Patient Record access intended for reviewing test patients, or investigating issues)
25	Super User	N/A		Super User	Level 5 - Super User	Common	Access to all System Functionality and all Data
26	Embedded Inbound SSO User	N/A		Embedded Inbound SSO User	Plus - Embedded Inbound	N/A	Added to any Embedded Users in addition to the above roles (usully Level 1 or Level 2 roles only), to prevent changing the password or moving out of patient context

Notes

* Registration Authorities and Smartcards: http://systems.digital.nhs.uk/rasmartcards (nrbacdatabase version 27.2 - National RA RBAC Database)

** See the ***CareCentric User Groups Functionality Permissions Summary*** for details on the FUNCTIONALITY permissions for each LEVEL

*** See the ***CareCentric Landing Page Tiles Summary Reference Guide*** to see which PATIENT DATA ACCESS is available for each landing page

CareCentric User Groups Functionality Permissions Summary

	Level 1	Level 2	Level 3	Level 4	Level 5
	Roles / User Groups: Admin/Clinical Support Clerical Receptionist	**Roles / User Groups:** Clinical Practitioner Community Mental Health Nurse Community Nurse General Practitioner GP Practice Manager Health Professional Medical Secretary Midwife Nurse Paramedic Pharmacist Psychiatrist Social Care Social Worker Unscheduled Care	**Roles / User Groups:** Audit Manager Caldicott Guardian Privacy Officer	**Roles / User Groups:** Systems Support	**Roles / User Groups:** Super User
All Users	Level 1	Level 2	Level 3	Level 4	Level 5
Can Search For Patients in Their Patient Groups	------>	------>	------>	------>	------>
Are asked for Patient Consent when entering the record	------>	------>	------>	------>	------>
Are shown alerts (on entering a patient record)	------>	------>	------>	------>	------>
Can Search For Patients outside their Patient Groups and tenancies (but **not enter the record**)	------>	------>	------>	------>	------>
Can access their own audit trail	------>	------>	------>	------>	------>
			Can search the system audit log / audit trail	------>	------>
			Can Export System Audit Trail	------>	------>
			Can Remove / Restore Documents, as needed (SysMan --> Document > Document Manager). Search for Documents by patient, Document type, date range	------>	------>
				Can revoke Patient Consent for a patient, user, or user group level	------>
				User Management	------>
				Access the **server email test page**, to test the server's ability to send email	------>
				Can access the System Status page	------>
					Can configure drop-down lists in ACDs (Data Capture Forms), where applicable
					Can adjust Consent Model settings
					Can manage Patient Groups in SysMan (used to control access to patients by specific users)
					Can manage lists of GP Practices

Note: This summarises access to SYSTEM FUNCTIONALITY permissions for each LEVEL.

Refer to the *CareCentric Landing Page Tiles Summary Reference Guides* to see which PATIENT DATA ACCESS is available, by default, for each User Group/ Role.

Appendix C - Fair Processing

Fair Processing will follow Article 13 and include information regarding:

- Identity and contact details of Data Controller/s and representatives
- Data Protection Officer contact details
- Purpose and Legal Basis for processing
- Recipients
- Transfers
- Retention
- Data subject rights, including access, rectification, erasure, restriction, object, portability and the right to withdraw consent
- Information regarding lodging a complaint with the Information Commissioners Office
- Whether there are any statutory or contractual requirements
- Automated decision making, logic behind it and any consequences

Fair Processing Campaign materials

Provided to all partners October 2019. Pack contains:

- One Health and Care A3 Poster
- One Health and Care leaflet
- Campaign Toolkit to support organisations to disperse campaign information
- One Health and Care Media Release
- One Health and Care banners/logos

One Health and
Care (Fair Processing

One Health and Care webpages, launched October 2019, an updated with the expansion of participating ICS orginanisations

https://www.twbstaffsandstoke.org.uk/about-us/our-work/one-health-and-care

https://www.stwics.org.uk/our-priorities/one-health-and-care/one-health-and-care-privacy-notice

https://www.blackcountryandwestbirmccg.nhs.uk/about-us/one-health-and-care

Demographic Analysis and Gap Analysis

ICR digital
programme - Demog

One Health and
Care Population Nu

Appendix D - Statutes and Key Principles

GMC and Caldicott Principles

Sharing of information should only be considered if it will improve the delivery of care **and** is necessary for direct care and that collaborative working should also mean formal arrangements are in place (signed information sharing agreements).[23]

Both the British Medical Association (BMA)[24] and General Medical Council[25] support the view that data should be shared between clinicians of patients in common. The GMC goes further, stating in their Good Medical Practice Code:[26]

> *44. You must contribute to the safe transfer of patients between healthcare providers and between health and social care providers. This means you must:*
>
> *a. share all relevant information with colleagues involved in your patients' care within and outside the team, including when you hand over care as you go off duty, when you delegate care or refer patients to other health or social care.*

This is reinforced following the creation of the seventh Caldicott Principle within the second Caldicott Review:

> ***7. The duty to share information can be as important as the duty to protect patient confidentiality.***

Health and social care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Digital Economy Act 2017

Section 35 of the DEA is regarding 'Disclosure of information to improve public service delivery'. A specified person may disclose information to another for the purposes of a jointly held objective. Schedule 4 of the Act includes 'Local Authorities' and 'a person providing services to a local authority' as a specified person. The principle being that information can be disclosed should it be for the purpose of improving the delivery of public services. This obviously needs to satisfy and take in to account Data Protection legislation. There are 3 conditions that need to be met:

> *Section 35 (9) (a) the objective has as its purpose the improvement or targeting of a public service provided to individuals or households, or (9) (b) the facilitation of the provision of a benefit (whether or not financial) to individuals or households.*

[23] *BMA Principles for sharing and accessing local shared electronic patient record*
[24] bma.org.uk/-/media/files/pdfs/practical%20advice%20at%20work/ethics/confidentialitytoolkit_card2.pdf
[25] http://www.gmc-uk.org/guidance/ethical_guidance/confidentiality.asp
[26] http://www.gmc-uk.org/guidance/good_medical_practice/continuity_care.asp

Section 35 (10) the objective has as its purpose the improvement of the well-being of individuals or households. This includes specifically under 11 (a) their physical and mental health and emotional well-being.

Section 35 (12) (a) the objective has as its purpose the supporting of the delivery of a specified person's functions, or (12) (b) the administration, monitoring or enforcement of a specified person's functions.[27]

The purpose of the ICR is to improve the provision of healthcare within the participating ICS regions. 'Benefit', as per Section 35 (9)(a), being for the good or advantage of an individual. The Act specifically states the improvement of physical and mental health wellbeing which an ICR could contribute to by improving the provision of care and support by the offering of a more joined up, effective and efficient health and care system.

Health and Social Care Act 2012 / Health and Social Care (Safety and Quality) Act 2015

Public sector organisations will derive their lawful powers through legislation that has created and established their remit. Changes brought about by the Health and Social Care Act 2012 and Care Act 2014 in April 2015 established the legal duty upon local authorities and health organisations to work together to integrate care. Some independent and Third Sector providers will have implied powers through contract arrangements made with public body commissioners.[28]

Health and Social Care (Safety and Quality) Act 2015 inserted sections 251A, B and C into the Health and Social Care Act 2012 places a legal duty on health and adult social care organisations to share information when it will facilitate care for an individual.[29] This is reinforced by Caldicott 2 as outlined under 2.5.1.

Legal basis has been strengthen by the Health and Social Care Act 2015 which gave statutory basis to the seventh Caldicott Principle 'the duty to share is as important as the duty to protect confidentiality' – so as long as the sharing is lawful we are legally required to share information to facilitate the provision of health/care services in the individuals best interests; however it must be ensured it is not what we project we think is the best interests of the service user.

Localism Act 2011 *Local Authorities*

The Localism Act by its very nature created space for local authorities to lead and innovate. Creating a regional ICR follows this mantra and allows the authority to the take control of decisions relating to the health and care of the people, where by improving services being provided. This includes working with health and creating a more efficient and effective care system with the aid of sharing records and creating systems to allow this all in the public interest.

Working Together to Safeguard Children 2018: Statutory Guidance

[27] https://www.gov.uk/government/publications/digital-economy-act-2017 Section 35 and Section 43, Code of Practice
[28] Sections 13N and 14Z1 of the National Health Service Act 2006 as inserted by the Health and Social Care Act 2012; and sections 3, 6 & 7 of the Care Act 2014.
[29] https://www.gov.uk/government/publications/review-of-data-security-consent-and-opt-outs page 24

The Government guidance and applies to all organisations and agencies who have functions relating to children.

Children Act 1989 and 2004

Places specific duties on organisations to co-operate in the interest of vulnerable children. The Children Act 1989 section 27 places a statutory duty on Health Professional to help Children's Social Care with their enquiries so long as it is compatible with their own statutory duties or other duties and obligations.

Section 10 of the Children Act (2004) requires each local authority to make arrangements to promote co-operation between the authority, each of the authority's relevant partners, and such other persons or bodies who exercise functions or are engaged in activities in relation to children in the local authority's area, as the authority considers appropriate. The arrangements are to be made with a view to improving the wellbeing of children in the authority's area – which includes protection from harm and neglect alongside other outcomes.

National Data Guardian Review for Health and Care 2016

This review was conducted by Dame Fiona Caldicott and focused on Data Security, Consent and Opt Outs. It focuses on safeguards of data but also highlights the expectation of the public that their data is shared across health and social care for their direct care.

> 'There continues to be a low level of public awareness and understanding of how health and social care information is used, but an expectation that information is shared for direct care'[30]

Recommendation 11 states 'There should be a new consent/opt-out model to allow people to opt-out of their personal confidential data being used for purposes beyond their direct care. This would apply unless there is a mandatory legal requirement or an overriding public interest.' NHS Digital have developed the 'opt out' system that will link into all relevant public bodies. It must be taken into consideration.

NHS Constitution 2015

The constitution states: 'You have the right to privacy and confidentiality and to expect the NHS to keep your confidential information safe and secure. You have the right to be informed about how your information is used. **You have the right to request that your confidential information is not used beyond your own care and treatment** and to have your objections considered, and where your wishes cannot be followed, to be told the reasons including the legal basis.'

Local Government Act 2000

http://www.legislation.gov.uk/ukpga/2000/22/section/2

Human Rights Act 1998

The Human Rights Act establishes the right to respect for private and family life, Article 8 (1) states 'Everyone has the right to respect for his private and family life, his home and his correspondence'. This is not an absolute right and is qualified by Article 8(2) 'there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic

[30] https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/535024/data-security-review.PDF page 24

society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others'. Current understanding is that compliance with the Data Protection Act and the common law of confidentiality should satisfy Human Rights requirements.

Justification and the social need for the ICR have been evaluated throughout this report. It is therefore perceived there will be no additional or new impact upon Article 8, the Right to Privacy.

Common Law Duty of Confidentiality

Although the legal basis under Data Protection Legislation is direct care the Common Law Duty of Confidentiality still stands. The Common Law has been developed from a series of court judgements and is an essential framework of law which must be applied. Under the Common Law Duty of Confidentiality information acquired by clinicians would be considered confidential. The general position is that where information is given in circumstance where duty of confidence applies the 4 bases (outlined below) should be taken into account.

1. With the consent of the individual concerned
2. Where there is a legal duty to do so, for example a court order
3. Justified in the public interest
4. There is a statutory duty that permits disclosure.[31]

'Consent' to meet the common law is different to, and should not be confused with, consent to process under Data Protection Legislation. Implied consent can be considered under the Common Law. Therefore the ICR meets those conditions. With the above justification in mind a 'consent process/screen' will not be used in the ICR. The common law cannot be considered in isolation, any disclosure must still satisfy any Data Protection law requirements.

A health or social care provider wishing to disclose personal data to anyone outside the direct care team however should first seek the consent of that service user. For secondary use of data the Common Law would be set aside only if the data was suitable de-identified.

[31] NHS Information Governance: Guidance on Legal and Professional Obligations, Department of Health