Privacy Impact Assessment Report

Document information

Title:	Privacy Impact Assessment Report
Project:	Cheshire Care Record (CCR)
Document owner(PM):	TBC
Document author:	[redacted]
Date created:	V3.0 FINAL
File name inc version:	DPIA Report - Cheshire Care Record REVISED – V3.0 FINAL January 2018

Version history and amendments are detailed in Appendix 1

Client contacts

Distributed to	Commented (Y/N)
Cheshire Care Record Governing Group (CCR IGG)	

Contents

1 Executive summary

This Data Protection (Privacy) Impact Assessment (DPIA) is a revised PIA as part of a review of the Cheshire Care Record programme's data sharing agreements and other documentation.

This report is intended to review existing risks and identify any further risks to this ongoing programme. This is done in the context of the changing data protection landscape with the introduction of the Data Protection Act 2018 and EU General Data Protection Regulation (GDPR).

A DPIA is intended to identify and manage risks relating to the rights and freedoms of natural persons taking into account the nature and purposes of processing. This allows the DPIA to document the identified risks, the likelihood and severity of those risks, particularly those deemed "high risk" and the recommendations and requirements to mitigate and manage the risks to provide assurance that the processing complies with the law.

Potential risks considered will include those identified at the last DPIA publication including the use of software systems that deliver CCR, and the organisational controls and processes that ensure the CCR is operated lawfully.

Some of these risk mitigations have been embodied in suggested amendments to the sharing agreement and contract, which is a separate document and are not entirely repeated here. Consultation and change control of the agreement must be a pre-condition before implementation for both existing and new signatories.

The revised DPIA and DPIA report is owned by the CCR Governing Group of Partner Organisations that are joint Data Controllers for the data processed through the Cheshire Care Record Information Sharing and Hosting Agreement.

The CCR is designed to support improved care delivery by providing multi-disciplinary care teams with a more complete view of the health and care history and current regime of a patient across multiple providers that support that person. CCR enables health and social care professionals to better collaborate, coordinate and safely transfer care where Partner Providers are engaged with people in common by facilitating the viewing of relevant information held by each. The point of care may include both immediate needs for past and current treatment information, i.e. in Accident and Emergency, or supporting collaboration for people with longer-term and more complex needs. This initiative is supported by Cheshire Pioneer and multi-professional guidance from the General Medical Council.[1]

The software that facilitates the CCR gathers service user information from different Partner systems into a central repository, where it is linked and held unseen until accessed by appropriately authorised system users. The partners to the CCR remain legally accountable (data controllers) for the information at all times and the arrangements are formalised through a legally binding contract, as is required by the Data Protection Act 2018 and EU GDPR.

This DPIA is reviewed and updated considering changes to legislation and the recommendations made in this DPIA are for consideration by the CCR Governing Group, and once agreed, circulated to Partner Organisations. Any risks identified should be considered, with responses determined by the

[1] http://www.gmc-uk.org/guidance/ethical_guidance/21187.asp

CCR Governing Group and actions arising for Partners Organisations implemented, where necessary, by their respective management and governance regimes.

Error! Reference source not found. brings together the recommendations and provides an o pportunity to record the CCR Governing Group's agreed responses. In addition, it is recommended that changes approved through the CCR Governing Group are appended to the DPIA, with their reasoning, for reference and incorporation in future iterations.

This document should be read in conjunction with the referenced materials, guidance, codes of practice and management contracts cited.

2 Introduction

A DPIA is a risk assessment and set of recommendations for the adoption of risk mitigating controls. DPIAs are typically amended during a project and, as such, should be considered a 'living' document that serves as a reminder of what has been considered and agreed, a reference point for review and a resource for future developments.

The DPIA helps to develop and communicate a common understanding of risk decisions and issues that have been addressed in the project with the objective of ensuring that appropriate measures are taken to safeguard personal and special category data. In this case, particularly any sensitive information about patients.

This DPIA has been commissioned to record the actions taken to ensure that Personal Confidential Data (PCD) will be appropriately accessed and processed, and to assist partner organisations to manage the implementation of the CCR locally. It provides recommendations which each Partner Organisation should follow to make sure it handles PCD appropriately, and that legal duties, such as the fair processing of data, are satisfied.

The DPIA report assesses and records the common understanding of the lawfulness and risk to the privacy of people whose Personal Confidential Data (PCD)[2] is shared between Partner Organisations listed in the contract**Error! Reference source not found.**.

In addition, the DPIA also allows Partner Organisations to demonstrate due diligence in ensuring risks to personal information are presented to appropriate internal governance bodies, and that they have been reviewed, accepted and will be monitored to ensure proposed risk mitigations are implemented and any residual risks managed. The ICO has been clear that they are less likely to take action, should an information loss or breach occur, if a DPIA has been completed.

The Information Commissioner's Office (ICO) publishes the Privacy Impact Assessment Code of Practice[3] alongside guidance from the Article 29 Working Party, the group which was the representative body for the EU before the GDPR came into force[4]

This DPIA has been redrafted from the original version to take into account the changes brought about by the introduction of the GDPR and Data Protection Act 2018[5], Risks have been introduced more explicitly to the DPIA to call out areas where resource may need more concentration and to highlight where changes may have occurred with the introduction of new legislation. The risk quantification is done using the NHS 5x5 Risk Matrix, and the risk score and colour attributed to each risk is subject to challenge by the group, change and subsequent approval based on their more detailed knowledge of the programme in its current form. Appendix 2 displays recommendations and risks together in tabular form.

---

[2] PCD is defined by the Information Governance Review (Caldicott 2) to encompass all states of personal data in health and social care: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/192572/2900774_InfoGovernance_accv2.pdf

[3] https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias/

[4] http://ec.europa.eu/newsroom/document.cfm?doc_id=47711

[5] http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

3 Audience

Partner Organisations' senior management who are accountable for information risk, and specifically each Partner Organisation's Senior Information Risk Owner (SIRO), Information Asset Owners and Caldicott Guardian (CG), or equivalents are the intended targets of this document. These may be the members of the Information Governance Group, who if different, are also an audience for the DPIA.

It is understood that the Information Governance Group for the CCR may not be meeting regularly. This is a group that is key to the management of confidentiality and data protection for the programme. Therefore, regular group meetings should be undertaken.

Recommendation 1: Communication of information risks and CCR Governing Group (Risk 1 – DPIA)

a. The CCR Governing group should be reviewed for attendance, reformed and formal dates set with standing agendas and a review of the terms of reference.
b. The group should be tasked with reviewing risks, assessing the risk scoring and each partner organisation including relevant risk into their information risks registers.
c. The CCR Governing Group should consider the risks identified, approve the mitigating controls and determine whether the residual risk level is acceptable. Where the remaining risk is unacceptable, the CCR Governing Group should agree what further risk-mitigating controls are required and implement a mechanism to ensure these are put in place[6]

RISK 1: HIGH

Governance of the programme is required and decision making, security and confidentiality must be a priority to provide assurances to the group members and, if necessary, assurances to the wider public and the regulator. There is a risk that the group not meeting properly in a structured manner means that any breach may not be handled properly and lead to serious criticism and reputational loss, along with potential higher fines.

[6] systems.hscic.gov.uk/infogov/security/risk/inforiskmgtgpg.pdf

4 System overview

The CCR system assists frontline care providers to make better informed care decisions about the appropriate care of a person by providing a view, often in their original (native) system, of information about the person they are caring for, derived from the systems of any partner organisation who has also cared for that person. CCR users continue to record their diagnosis, decisions and activity in their native system.

The software that has provided the operational platform, since the launch of CCR is the Graphnet CareCentric[7] interoperability system.

The CareCentric system takes data from partner systems in almost any format and frequency, links the data, using the NHS Number as the common linking identifier, and displays it back to users, subject to access controls that ensure only appropriate data is displayed (Role-Based Access Controls – RBAC) and that this is only to users who are caring for the person whose record is being viewed (Legitimate Relationship control – LR).

The CCR system records everything a user has viewed in an audit trail. The audit trail can be viewed by system users. If there is an issue, the audit trail can be viewed to establish what a user could see when viewing a record. Users with appropriate RBAC controls can also view and report on who has looked at a person's record, and what records have been viewed. This can be provided to the person on request.

These controls support compliance with commitments made to NHS patients in the NHS Constitution[8] and Department of Health information strategy[9] as well as obligations in law.

More detailed controls in the CareCentric system are explained in the appropriate sections below along with any recommendations and risks identified.

[7] www.graphnethealth.com/
[8] www.gov.uk/government/uploads/system/uploads/attachment_data/file/170656/NHS_Constitution.pdf
[9] www.gov.uk/government/uploads/system/uploads/attachment_data/file/213689/dh_134205.pdf

5 Data Controller/Data Processor

Previously the programme recognised that partner organisations in the CCR programme would be data controllers "in-common". However, this is no longer the case.

Under GDPR and the Data Protection Act 2018 the concept of "in-common" no longer applies and is replaced by new definition. Article 4(7) of the GDPR[10] defines a controller as:

> '…[a] body which, alone or jointly with others, determines the purposes and means of the processing of personal data…'

Whilst there is a definition change, the practical application of controllership does not change substantially except to impose a new level of liability on all parties.

Previously, as Data Controllers in-common, each partner organisation processes data from a common pool, but determines how this is used in their own organisation, within the contractual terms, but otherwise without control of another body. This limited the likely liability in the event of a breach to the particular controller acting "on their own".

However, under the new legislation data controllers acting jointly may be subject to extra liability as a group due to the "joint" nature of the activities. It will therefore be important to ensure that contracts and agreements reflect this new status and explicitly state the expected liabilities of all parties in circumstances where personal data breaches occur or other "misuse" of personal data takes place.

Data controllers appointing data processors must abide by the requirements in the GDPR. Article 28(1) states:

> 'Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject…'

The new legislation does not change the definition of a data processor:

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

However, new requirements are placed on data processors which imposes some liability in the event of a personal data breach. Together with the assurances that must now be provided, this places extra requirements on both controllers and processors and defines a new risk in terms of ensuring adequate measures to secure personal data.

There has been no change in how the CCR data and software are hosted by the Countess of Chester Hospital NHS Foundation Trust (COCH); COCH is the Data Processor contracted through the contract. COCH is also a Data Controller in its own right and a full Partner Organisation in the contract.

[10] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

These requirements, as did the DPA 1998 legislation before it, are central to the revision of the data sharing agreement.

Recommendation 2: Contracts and agreements review (Risk 2 – DPIA)

Contracts and sharing agreements between all involved parties should be reviewed and updated to reflect new legislative requirements.

RISK 2: MEDIUM HIGH

Contracts that are no longer fit for purpose represent a risk in that parts of the documents may be no longer reliable in the case of a dispute. In the case of a data processor contract being invalidated, this defaults the processor to a data controller. Risks related to a failure based on contractual requirements can be mitigated, largely by a formal review and where necessary new or amended contracts and agreements.

6 Data Flows & Record of Processing

The mapping of data flows as part of the DPIA process was recommended in the DPA 1998 based guidance on PIAs from the Information Commissioner. This recommendation has not changed, and has been strengthened by the introduction of the "Records of Processing", which is detailed in Article 30 of the GDPR, and lists requirements that amount to a data map of personal data:

> 'Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:
>
> (a) the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
> (b) the purposes of the processing;
> (c) a description of the categories of data subjects and of the categories of personal data;
> (d) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
> (e) where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
> (f) where possible, the envisaged time limits for erasure of the different categories of data;
> (g) where possible, a general description of the technical and organisational security measures referred to in Article 32(1).'

In addition, there are records of processing requirements related to data processors in Article 30 which data controllers will need assurances from processors that the required information is recorded and managed appropriately.

The contract will limit what data flows the Data Processor may allow in and out of the system and the purposes for which the Data Processor and in-common Data Controller parties are allowed contractually (and legally) to access and process this data. The following flows of PCD have been allowed in contract and are considered for the purposes of the original DPA. A review of these for current relevance will be required.

Flows of Personal Confidential Data:

1. From each partner in to the CCR system
2. At rest in the COCH datacentre where the CCR system is hosted
3. Each access of PCD through the CCR system by the Data Controllers in-common
4. For the purpose of de-identification by COCH instructed by the CCR Governing Group.

Flows of de-identified data:

1. If data is 'de-identified' so that a person can no longer be identified without unexpected effort, the data is no longer personal data. This data would be used by care organisations and care commissioners to monitor, assess and report on local services. People should still be told their information is being used in this way.

Recommendation 3: Management of data flows (Risk 3 – DPIA)

The management of data flows is important as it relates directly to the Records of Processing requirements, providing a basis for managing flows and understanding what categories of data etc., are being processed.

A tool to help manage this process is recommended, so that changes to processing flows and types can be reflected swiftly and with lower management resource impact.

Regardless of whether a tool is used, the records of processing must be in a reasonable state as it may be requested by the ICO at any time. Failure to supply such information in a timely manner will at best bring criticism and at worse cause action to be taken against data controllers.

All controllers must themselves create and manage a record of processing. A consistent approach to this will make creation of a CCR flows/map easier.

RISK 3: MEDIUM HIGH
A lack of good records of processing information and data mapping leaves organisations open to criticism and more punitive action, in the event of a data breach. Understanding the information flowing through systems and organisations is a fundamental part of information management.

CCR is a 'view only' system – users can read information from other systems but can only write to their own (native) system. No user in one organisation will be able to change a record in another, and therefore no further flows are created. However, as health requirements change there may be a need to consider how the CCR may function in a way that enables coordinated care plans and other care processes and pathways, to be managed across the CCR population.

Recommendation 4: Future need for closer integration (Risk 1 – DPIA)

It should be recognised that, as integrated health and social care matures, future uses of the CCR system may require coordinated care plans to which multiple providers contribute. The CCR Governing Group will need to commission an in-depth review of the agreement/contract and PIA should this eventuality arise as it may require a considerable change. Such a change would require extensive stakeholder engagement and a consideration of the possible requirement of consent.

RISK 4: MEDIUM LOW

The ability of the CCR Governance Group to assess and review potential helpful changes and decide on how the CCR, if at all, can be used is important to the future development and use of the CCR. Not building such processes into the Governance Group risks the system becoming less effective in areas of growth in the health sector.

7 Data protection principles (Revised)

The eight data protection principles of the Data Protection Act 1998 have been replaced by six principles under the GDPR and adopted by the Data Protection Act 2018.

A DPIA reconsiders:

1. Extent to which the privacy of a data subject is affected by the new proposed use of their data, e.g. a loss of privacy due to changes in the manner and purpose of processing
2. Risk of causing substantial damage or substantial distress to the data subject through the new proposed use of their data
3. The risk of a loss of control of the data
4. The risk of inappropriate data access maliciously or unintentionally
5. The risk of data corruption
6. The risk of non-compliance with the Act and/or Regulation, including reputational and financial consequences.

For reference, the six revised principles which can be found in Article 5 of the GDPR[11]. Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject (**'lawfulness, fairness and transparency'**);
(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, in accordance with Article 89(1), not be considered to be incompatible with the initial purposes (**'purpose limitation'**);
(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**'data minimisation'**);
(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'**);
(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…(**'storage limitation'**);
(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 (**'integrity and confidentiality'**).

It is also stated in Article 5 that data controllers 'shall be responsible for and be able to demonstrate compliance with [the above principles]'. This is **'accountability'**.

[11] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

7.1 Principle (a)

(a) Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')

How the CCR complies with this principle:

Lawfulness
For each purpose the data is processed, there must be a basis in law. The Data Protection Act 1998, and by inference the new legislation, has been extended by case law to include the Human Rights Act 1998 article 8 (right to privacy) and the Common Law Duty of Confidentiality (CLDC). It is necessary to satisfy the CLDC as well as the GDPR/DPA2018. CLDC applies to the expected use of information given in confidence. It is generally accepted that, if the processing is fair, and the Data Controller can respond to requests to cease processing, if required, then processing is lawful.

Fairness and lawfulness should not be confused with consent, which may be a condition for processing special categories of personal data.

Under the new legislation, the lawfulness of processing data changes very slightly and is listed in both Article 6 of the GDPR, Lawfulness of processing and Article 9 of the GDPR, Processing of special categories of personal data.

Article 6 requires one of the following to be applicable for processing personal data:

(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(c) processing is necessary for compliance with a legal obligation to which the controller is subject;
(d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
(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;
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) does not apply to processing carried out by public authorities in the performance of their tasks.

Since the initial introduction of the CCR, the understanding of consent requirements for sharing for care have changed with consent now being a lawful basis that should not be relied upon in the context of sharing for care purposes.

The BMA states:

> *'In the absence of evidence to the contrary, patients are normally considered to have given implied consent for the use of their information by health professionals for the*

purpose of the care they receive. Information sharing in this context is acceptable to the extent that health professionals share what is necessary and relevant for patient care on a 'need to know' basis. (BMA, Card 2)'[12]

Guidance provided by NHS Digital states:

'All health and adult social care organisations must, by law, share information with each other about patients they are caring for directly, to improve the care provided. They must also use a patient's NHS number as a consistent identifier when sharing data or information about them. This was set out in the Health and Social Care (Safety and Quality) Act 2015, which aimed to reduce anxiety about data sharing. The 2013 Caldicott Review found that in some cases this anxiety meant patient information was not shared, even when sharing would have been in the best interest of the patient.'[13]

The Health and social Care (Safety and Quality) Act 2015[14] which has been enacted since the original CCR programme was delivered, means that sharing to care is now seen as fundamental to NHS patient care. However, it does not remove any rights an individual may have to refuse to have their information shared.

Article 9: Processing of special categories of personal data

Previously known as sensitive personal data, the GDPR and DPA 2018 use the term "special categories". Data concerning health, now including genetic and biometric data are termed as special category data.

Again, multiple bases for lawful sharing are listed in Article 9 and of these, the following are of relevance:

- The data subject has give explicit consent to the processing of personal data for one or more specified purposes;
- The processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
- The processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, **the provision of health or social care or treatment or the management of health or social care systems and services**…

For all flows of PCD, CCR is relying on having a medical purpose (often referred to as 'direct care') to satisfy the legal basis for processing. This purpose is supported by the guidance from the BMA and GMC quoted above and these have been clarified by the seventh Caldicott principle[15]. This is not independent of the other conditions, especially the communications necessary to satisfy the CLDC, fairness and the Human Rights Act.

[12] bma.org.uk/practical-support-at-work/ethics/confidentiality-tool-kit

[13] https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/information-governance-alliance-iga/information-governance-resources/information-sharing-resources

[14] http://www.legislation.gov.uk/ukpga/2015/28/contents/enacted

[15] www.gov.uk/government/uploads/system/uploads/attachment_data/file/251750/9731-2901141-TSO-Caldicott-Government_Response_ACCESSIBLE.PDF

Under the update legislative requirements, the need to request explicit consent is no longer relevant, with law and standards reflecting an implied consent approach under the common law duty of confidence. Whilst still in place, the CCR Governing Group are reviewing this process with the intention of ensuring that future processes comply with accepted practice.

The CCR currently exceeds the minimum standards of law by also requiring explicit consent to view the first time shared information (see Figure 1 Consent process flow) where the patient has capacity. If the patient lacks capacity and this has been determined by a health and social care professional in accordance with the requirements of the Mental Capacity Act 2005, the system allows the clinician to access the shared record, but also sends an alert to ensure all such accesses are reviewed for appropriateness.

Further, people who are engaged with multiple care providers, when consulted, have expressed the view that they do not wish to go through the consenting process at every access where they are present. They have the option to set a longer period of consent in the system. This may be reset if there are changes to the use of the data agreed by the CCR Governing Board, for example a new organisation joins, or if the CCR Governing Board sets a time limit, e.g. requiring re-consenting annually.

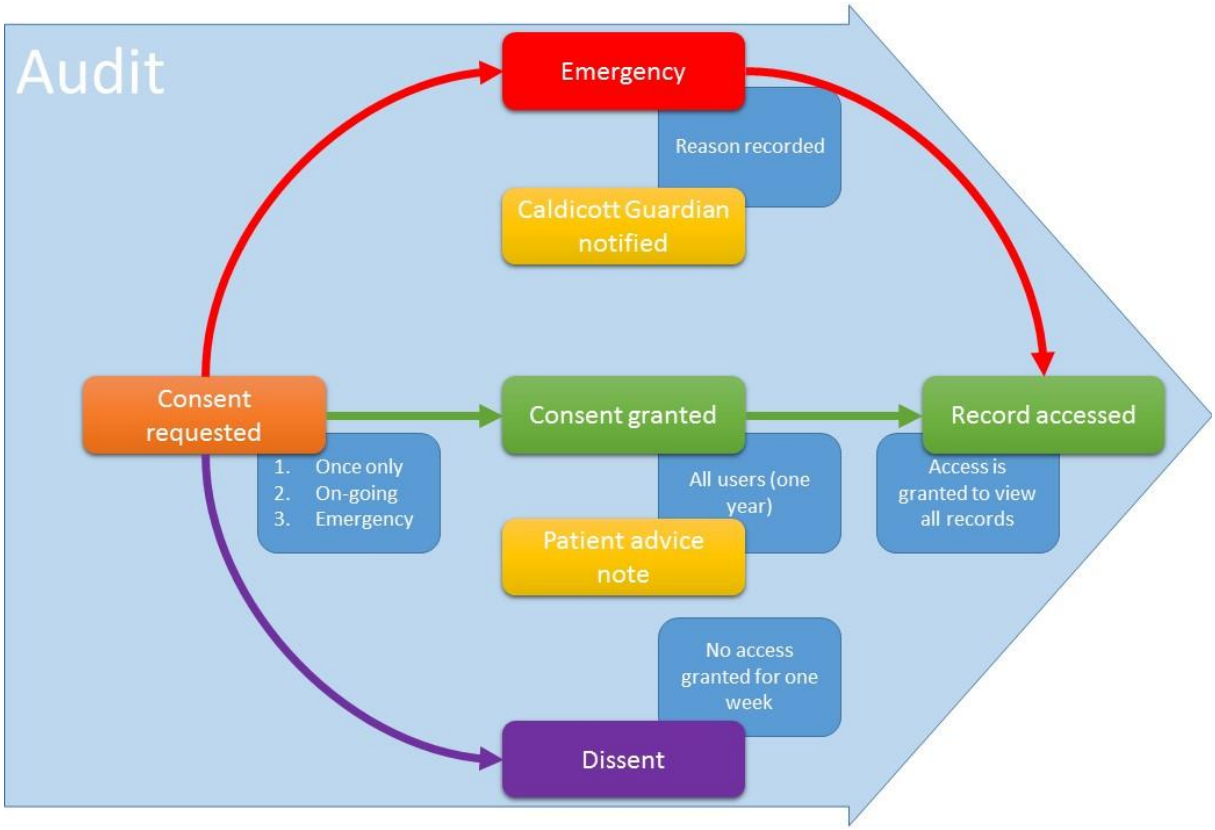

Figure 1 Consent process flow

To obtain consent when the patient is present and has capacity, professionals accessing the shared record must read the following statement and be assured that they understand and accept that their information is being accessed. This is recorded by that professional in the system:

If you give consent, you are allowing all health and social care professionals within Cheshire who treat you to access your shared record when needed to support the delivery of your personal care for a year. This will include hospital, GP, mental health, community and social care teams. You can ask your GP to remove the consent at any time.

Note, as stated in section 4 System overview, the system forces explicit consent to view in the operation of the system:

- CCR will primarily be launched from within the clinical system or social care system of the participating organisation, enforcing the requirement for a legitimate relationship to exist between the patient and the professional prior to reviewing the record. This is subject to exceptions.
- Patient consent to view is always discussed at first view of the data, and the patient is given the option to consent or dissent.

As the system use matures, it is likely that further use cases will develop and the CCR Governing Group will be asked to review access arrangements, for example when patients are referred by one health and social care professional to another for treatment, which would be approved by the patient in advance, rather than spending time summarising the record, the receiving health and social care professional may access the CCR. Similarly, where patients are referred for mental health services, it is common to access the record in advance of the first meeting. Indeed, some patient groups have expressed the view that it should be compulsory for health and social care professionals to familiarise themselves with the patient history and current regime before seeing them.

Dissent

Dissent to sharing of information must be respected and managed as part of the CCR system. Since 2018 the National Data Opt-Out Programme provides a national database of individuals' who have expressed a wish to not have their personal data shared for **non-care purposes**. However, at the present time the CCR programme collects personal data for care purposes only and this dissent management must be part of the systems, in order to provide consistent management and comply with data protection legislation and NHS guidance.

Recommendation 5: Patient Objection Management Systems (Risk 4 – DPIA)

The CCR Governance Group will need to consider how dissent will be managed, in future. Many similar initiatives now remove the requirement for consent, but do allow (as is their right) the ability of patients to object to sharing taking place. The collection of consent adds complexity to the delivery model and the management of patient information. It is important the pros and cons are considered and discussed in light of the changes to the consent landscape and decisions made on how the management of patient objections might be managed in the future.

RISK 5: HIGH

As the sharing of information grows, a model which is out of step with other initiatives will create issues in joined up care in the future. It is important that the CCR programme balances new ways of working with patient rights and what changes can be implemented locally, whilst considering the future uses of the data held, for care purposes.

Fairness
It has been established by case precedent that 'fairness' in the first data protection principle encompasses the common law duty of confidence. For the data processing to be fair, the proposed use must be expected by the data subject. To achieve this, the use(s) must have been effectively communicated – for which there is no test of reasonableness as to how much effort must be made in this communication – although it is generally accepted that the more unexpected and sensitive the data, the more effort must be made in ensuring data subjects are aware. This declaration of proposed use and supporting information is known as a Privacy Notice), but this is only one method and all available channels of communication should be considered.

Each Data Controller continues to have an individual duty to communicate their Privacy Notice to patients and service users. The use of various media was suggested, such as posters, leaflets, webpages et al. With the service in operation, it is necessary to review the content of communications and provide updates, where necessary, for individuals so that they can be made aware of changes that have taken place. This may be minor changes to frontline posters and leaflets, but more change where individuals may seek further information and guidance, such as on webpages. Reference to ICO public guidance would also be a consideration and help with transparency and verification that the processes being undertaken are fair and lawful.

The programme runs a website[16] which contains very useful, well thought through information for patients. However, it has some areas that are now out of date, and a review of this information will be needed. This can only be performed once the CCR Governing Group have made decisions on the recommendations in this report and in light of the new data protection legislation.

Recommendation 6: Review of patient information (Risk 5 – DPIA)

Review of existing patient information should be repeated to ensure inclusion of GDPR references and changes to individuals rights and freedoms along with references to outside, valid guidance. Currently information refers to consent, and whilst this might continue, it requires a full review and consideration of new ways of working and then these decisions being reflected in communications materials.

RISK 6: HIGH

It is important that communications and fair processing is kept up to date to manage risks related to patients failing to be adequately informed, and subsequent investigation by the ICO leading to criticism and the potential loss of trust in the system.

The BMA Confidentiality Toolkit Card 2 further clarifies the connection between fairness, consent and communication:

> *'Health professionals bear responsibility for the disclosures they make, so when consent is taken to be implied, they must be able to demonstrate that the assumption of consent was made in good faith and based on **good information**.*

[16] https://www.cheshirecarerecord.co.uk/

If not, it is no consent at all and some other justification will be needed for its disclosure.'

The collaborative documentation for patients will be reviewed to ensure it is still fit for purpose including the relevant documents list in Appendix 2 and the CCR Privacy Notice latest version.

This will enable changes to be made that support the call for consistent messaging across multiple organisations, ensuring that the current messages relating to explanation of the purpose for the system, what information will be shared, and how people can opt out of sharing their information if they so wish (see later notes on consent and dissent, below).

Recommendation 7: Review Communications to hard to reach groups (Risk 5 – DPIA)

Ensure that the materials and communication channels are still in effect, to reach the entire population to support implied consent with consideration for a further equality and diversity assessment to ensure that effective communications reach the harder to reach groups.

RISK 7: HIGH
Assuming that action was taken at the launch of the CCR to include hard to reach groups, then this review will help to mitigate a medium-low risk that these channels are not still operating and that it may lead to complaints.

7.2 Principle (b)

(b) Personal data shall be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes… ('purpose limitation')

How the CCR complies with this principle
From the previous legal regime to the introduction of the GDPR and DPA 2018, there is not a significant change that affects this principle, previously Principle 2.

However, the purposes of processing must still be noted in the ICO Registration for each partner and be wholly compatible with the fair processing information that has been provided to patients and service users in the privacy notice and associated information.

It is unlikely that the programme will need to consider a public communications campaign as was implemented during the original launch and the changes may be seen as an update to the information of which patients and service users should be aware.

There is still a requirement that all organisations must be registered with the ICO as Data Controllers and that the data processor (the Countess of Chester Hospital NHS Foundation Trust) will be restricted in contract to process data only on behalf of the Data Controllers.

It is a good opportunity for all data controllers to review their registrations, if not already done.

Recommendation 8: Partner Organisations review their ICO registration and include any new purposes (Not reflected in DPIA)

Review the purposes and make suitable changes in light of the GDPR changes where there may be a change in data processed. This will help as evidence of due diligence for each data controller.

RISK 8: LOW

It is understood that all partners have registrations in place and that a review would promote good practice. There is little risk if this is not carried out but could potentially lead to the ICO requiring a registration to be updated if thought to be inaccurate or out-of-date.

7.3 Principle (c)

(c) Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (**'data minimisation'**)

How the CCR complies with this principle

The limitation of PCD use remains similar to how the programme has managed this use, previously.

The legal basis for processing (Principle (a)) must still be considered and how data can be managed to ensure that only that information which is required for the performance of the task, is accessible and used.

In the context of medical records this is sometimes harder to achieve as the relevance of particular medical notes may/or may not have relevance to the here and now. Only a medical professional can make that judgement. However, with the management of the data in the systems and the consent of patients for the sharing of their PCD, this provide a context and enabler to allow the PCD to be used.

Reminding staff of the Caldicott principles and ensuring that IG training is up to date at all times will also help to provide risk reduction and assurance that staff understand their obligations under this and the other Principles.

Recommendation 9: Confirm that training for health and social care professionals in IG is up to date and that they are informed of the CCR and its uses including the management of data flows (Risk 6 – DPIA)

Reconfirm that each partner organisation is continuing to ensure staff are adequately trained and that health and social care professionals using the CCR have training to identify and manage data flows so that they can review these flows regularly.

RISK 9: MEDIUM-LOW

This risk is linked to Recommendation 3 as it is important in the context of training that data flows are managed and recorded effectively. Health and social care professionals using a tool to manage the data flows will be able to review theirs and others to ensure no conflicts. Failure to do this risks data flows not being managed properly and data transferring to place it may not be sanctioned for.

7.4 Principle (d)

(d) Personal data shall be 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').

How the CCR complies with this principle
Data in CCR will be as accurate as the data in the source systems.

It is incumbent on all Data Controllers to have in place data quality processes that, as far as is practicable, provide assurances that the data being processed into the CCR is accurate and up-to-date and that where information is found to be of questionable quality, suitable actions are taken to ensure correction or management of the data to improve the accuracy and timeliness of the data.

Recommendation 10: Data Quality procedures (Risk 10 – DPIA)

The CCR Governing Group should establish, or re-engage, a sub-group to either coordinate Partner Organisation reporting of discrepancies in the data, or design processes for adoption by all Partners to address data quality issues. These are inevitable and could be a clinical risk if the differences are not understood.

Whatever strategy is adopted, it must consider training for staff in how to respond to seeing discrepancies in the record.

Risk 10: HIGH

Clinical inaccuracies, or differences may lead to individuals' being treated with information that is not fit for purpose and may delay or complicate treatment or potentially ultimately cause death.

7.5 Principle (e)

(e) Personal shall be 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… ('storage limitation).

How the CCR complies with this principle
Each organisation will have its own retention schedules for electronic data it keeps about individuals, normally in accordance with Appendix 3 of the Records Management Code of Practice for Health and Social Care.[17] The current method used by the CCR whereby each daily extract updates the data already held within the CCR, overwriting data that has changed, along with an audit trail of access enable this Principle to be complied with.

In the new Code of Practice, published in 2016, reference to electronic data and audit trails being retained indefinitely has been modified, stating

[17] https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016

'The amount of work required to maintain digital information as an authentic record must not be underestimated. For example, the information recorded on an electronic health record system may need to be accessible in 100 years (including an audit trail to show lawful access and maintain authenticity) to support continuity of care.'

Audit trails will be kept substantiating the access to records, but due to the nature of the storage of the records not being within the CCR, the retention still applies only to audit trails.

Recommendation 11: Storage in CCR system (Risk 12 – DPIA)

The use of Graphnet hosted on a local system at Countess of Chester Hospital (COCH), brings with it some risks in terms of ensuring continued security and confidentiality and long-term access to the system should the Hospital cease, or pull out of the CCR. A review of the appropriateness of local storage and the agreements in place is recommended.

A review of retention and storage policies and processes should be undertaken, with any concerns of changes being reflected in planned modifications to ensure the continued good working of the systems.

RISK 11: MEDIUM-HIGH

With local storage it is important that security set up and confidentiality are maintained to manage the risks related to information being available locally where it shouldn't be and to manage potential intrusions into the hosting systems.

Statistical data, which is de-identified and therefore not subject to privacy legislation, is not relevant to this process or within the scope of this DPIA,

7.6 Principle (f)

(f) Personal data shall be 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 ('integrity and confidentiality').

Requirements for securing personal and special category data are enshrined in the sixth principle of the GDPR, and reinforced through the requirements of the Data Security and Protection Toolkit and NHS policy. Serious breaches of the GDPR can result in a fine of up to €20m or 4% of global turnover. In practice however, fines are likely to be proportionate to the breach incurred and the size of the business. Nevertheless, potential financial action by the regulator now carries a far greater monetary value.

Equally, if not more, significant is the potential reputational damage that may be incurred through loss of trust with patients and service users. This could lead to care quality being compromised and other action via other NHS regulatory organisations.

The GDPR Article 32 'Security of processing" provides several paragraphs which set out the conditions under which data must be protected.

Paragraph 1 states:

> 'Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:
>
> (a) the pseudonymisation and encryption of personal data;
> (b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
> (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;
> (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.'

It is highly likely that existing technical and organisational measures remain fit for purpose under the GDPR and DPA2018. Reviewing the mechanisms employed for security measures including consideration of a penetration test now that the system has been in operation for several years will aid in the assurances that must be provided to the regulator and to the public.

Recommendation 12: IT Security Review (Risk 8 & 9 – DPIA)

Locally held systems will need to have assurances and evidence that IT security is of a standard acceptable to the CCR Governing Group and that there is compliance with required standards.

A penetration test and report on the IT Security of the Graphnet system and the data flows will ensure that the security remains fit for purpose.

RISK 12: HIGH

There is always a risk related to IT security and unauthorised accesses to systems. This risk can be reduced through the application of good testing including formal penetration testing and reporting of the standards used to secure the system and clarification that the system is as robust as possible.

Paragraph 2 states:

> 'In assessing the appropriate level of security account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to personal data transmitted, stored or otherwise processed.'

The data in CCR is sensitive (special category) data and must have commensurate security measures. Employing industry standard techniques and tools and ensuring regular review of actively managed risks is a requirement to demonstrate the level of due diligence that is expected for special category data.

> **'**Adherence to an approved code of conduct as referred to in Article 40 or an approved certification mechanism as referred to in Article 42 may be used as an element by which to demonstrate compliance with the requirements set out in paragraph 1 of this Article.'

The NHS places requirements by virtue of the IG Toolkit (now the Data Security and Protection Toolkit) and at the time of writing there are no external codes of conduct or certification that is relevant to this programme.

Paragraph 4 states:

> **'**The controller and processor shall take steps to ensure that any natural person acting under the authority of the controller or the processor who has access to personal data does not process them except on instructions from the controller, unless he or she is required to do so by Union or Member State law.'

Ensuring that roll-based access is in place and a rigorous process for adding and removing people from access to the system should be in place. A review of this activity is recommended so that the organisations involved can be assured that themselves and partners are complying with security requirements and that processes are robust.

Previous to the implementation of the GDPR and DPA 2018 data processors were bound by contract only, having no statutory duties under the DPA 1998. This has now changed, placing duties on data processors as well as data controllers, with the controllers having duty of due diligence with respect to the processors they contract; '*Where processing is to be carried out on behalf of a controller, the controller shall use only processors providing sufficient guarantees to implement appropriate technical and organisational measures*…'

There is therefore a need for the Data Controllers to ensure contracts are relevant and fit for purpose and that assurances given by Data Processors are acceptable.

Access control

Role based access controls are in place. However, it is a good point in time to review the processes for enabling and revoking access and that administrators assigned by Data Controller are up to date.

Recommendation 13: Access controls and user profiles (Risk 7 – DPIA)

All organisations should review their procedures and ensure that a member of staff is allocated as the system administrator and take part in appropriate training in order to ensure that appropriate user profiles are allocated. Similarly, procedures must be in place to ensure users are removed from the system access if they no longer have legitimate access. Role based access schedules need to be in place to ensure that only those people with legitimate business need can access what they require to do their roles.

RISK 13: MEDIUM-HIGH

Access to systems must be controlled with authorised staff only being allowed access to the system. They must be managed in a way that ensures they are added correctly and removed when the time comes, and their access is commensurate with the role they perform. Failure to manage this process properly risks access by individuals who have no rights to be there and a potential breach of confidentiality and security which in turn may be reportable as a data breach to the ICO.

How the CCR complies with this requirement

Contractual arrangements should be reviewed, along with the assurances and evidence provided by each party in respect of complying with contractual obligations.
The overall content recommendations of a contract are largely unchanged. However, the changes to Data Processor liabilities and data subject rights means that reviewing the contract is an important factor in ensuring that the relationship definitions are fit for purposes.

A summary of the key areas initially coming from the Information Governance Review[18] are:

- Definition of the Data Controller and Processor
- Limiting the Data Processor to only act on the instructions of the Data Controller
- Definition of the data which are to be processed, and restrictions on the use of that data without further instruction from the Data Controller
- Restrictions on the territorial limits of the data at rest
- Definitions of the expected security arrangements for the data
- Definitions of the expected security accreditations to be held and maintained by the Data Processor
- Reporting and management of serious incidents and reporting
- Requirement to be subject to audit and to share that audit data with the Data Controller.

Refining this content to ensure compliance with GDPR requirements and to avoid any contradictions between the old legislation and the new should be a priority.

8 Data Subject Rights

A central tenet of the GDPR relates to the changes to data subject rights. Whilst a significant part of the rights remain very similar, there are changes that support greater power of the individual to have more control over their personal data.

The rights are summarised below.

8.1 Article 12 – Transparency

This article relates to the controller taking appropriate measures to provide specific information held about individuals, the content of which is listed in Articles 13 & 14.

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

In effect it places an expectation on Data Controllers to honour Subject Access Requests (requests for personal information) and limits the response time to one month, previously forty calendar days, with certain exceptions.

How the CCR complies with this principle

Each Data Controller will handle requests for copies of information held on an individual basis, and will not use the CCR system to support Subject Access Requests, but should refer patients to the respective Data Controllers. This is because a contributing organisation may know of a constraint on releasing certain information that may cause damage or distress to the person, such as mental health data.

The GDPR Article 23 provides restrictions that may be applied to the rights of data subjects in that information need not be disclosed if it would be likely to cause serious harm to the physical or mental health of the Data Subject or any other person.

The NHS Constitution requires that dissent to share is respected and therefore the extract process will ignore patients with a specific system code or 'READ CODE' in their record.

Appendix 3, includes information about the codes to be used by GPs in this event and this will then trigger denied access to any information from any sources within CCR. Other organisation types will have local system-specific processes to respect dissent to share.

8.2 Articles 13 & 14 – Information to be provided

Articles 13 & 14 of the GDPR cover information to be provided where personal data are collected from the data subject. (Article 13), and information to be provided where personal data have not been collected from the data subject, (Article 14).

The requirements of information to be provided are listed in the Articles. However, this DPIA calls to attention the 'information… the controller shall, at the time when personal data are obtained, provide the data subject with the following [to] ensure fair and transparent processing:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) the existence of the right to request from the controller access to and rectification or erasure of personal data or restriction of processing concerning the data subject or to object to processing as well as the right to data portability;

(c) where the processing is based on point (a) of Article 6(1) or point (a) of Article 9(2), the existence of the right to withdraw consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal;

(d) the right to lodge a complaint with a supervisory authority;

(e) whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is

obliged to provide the personal data and of the possible consequences of failure to provide such data;

(f) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

How the CCR complies with this requirement

There exists documentation in the form of web pages, leaflets and posters that inform the public of the way their information will be used and shared for their direct care under the CCR programme. Reflecting as much of the information called out, above in these communications will ensure that the public have amp[le opportunity to see, read and if they wish, question the use of their personal data.

This information will need to be assessed, and communications reviewed, to ensure that the fairness and transparency requirements are met when supplying patients and service users with fair processing notices.

8.3 Article 15 – Right of Access

This Article enshrines an individual's rights to be able to obtain from a data controller confirmation regarding the processing of their personal data and if that is the case, access to the personal data and additional information. This links closely with Article 12 (section 8.1).

How the CCR complies with this requirement

As previously mentioned, the act of complying with Subject Access Requests and ensuring that individuals can request their data is in place and simply needs reviewing to ensure that the processes remain robust.

8.4 Article 16 – Right to Rectification

The right to rectification is not a new right and remains unchanged from the DPA 1998. An individual if noticing errors or omissions, makes contact to request their records to be updated, then the data controllers concerned will manage this through their usual processes.

Medical records cannot normally be rectified with approval, usually of (at least) the Caldicott Guardian and existing processes should be adequate to continue this.

How the CCR complies with this requirement

Each Data Controller handles requests for copies of information held on an individual basis, and will similarly handle any requests for rectification through their existing processes. The CCR system is not used to support these changes.

8.5 Article 17 – Right to Erasure ('Right to be Forgotten)

This new right is a qualified right and will only be granted if there are no other overriding reasons to keep the information requested to be erased.

How the CCR complies with this requirement

The decision to accede to such a request will be a decision to be made by individual controllers, outwith their involvement in the CCR as each data controller will need to determine the reasonableness of such requests and remove information from their systems. This right will therefore sit outside the CCR.

8.6 Article 18 – Right to Restriction of Processing

Should one of the following apply, the individual will have a right to request that the data controller restrict processing:

(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;

(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;

(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;

(d) the data subject has objected to processing (see Article 21) pending the verification whether the legitimate grounds of the controller override those of the data subject.

How the CCR complies with this requirement

As with other rights, the data controller will be acting in isolation from the CCR as the organisation to which an individual has made a request. As each data controller maintains their patients' information independently, any restriction aimed a data controller will be dealt with by the controller specifically named by the request.

8.7 Article 19 – Notification of Rectification, Erasure or Restriction

This right states an explicit requirement that a data controller informs an individual who has requested rectification, erasure or restriction of processing, that they must inform each recipient of the personal data in question that such a process has taken place.

This will mean that a data controller in the CCR programme will need to inform partners to whom the data has been disclosed, in practicality all data controllers so that they are aware of changes and can take decisions themselves on the data they hold, or be aware that an individual may request similar services from them.

How the CCR complies with this requirement

To comply with this Article the governance group should be used to regularly report such activity and distribute the activities to all partners so that there is a central source.

8.8 Article 20 – Right to Data Portability

Data portability enables an individual to receive personal data which they have provided to the data controller. This information is to be received in a structured, commonly used and machine-readable format. They also have the right to give the data to another data controller.

There are conditions attached which means that the processing must be based on consent for both personal data and special category data or on a contractual basis. Furthermore, the processing is carried out by automated means.

How the CCR complies with this requirement

Individuals will have a right to request such information from a data controller and the CCR operates in a way that this information will not come from this system, but be provided, if relevant, by an individual controller to whom the request has been made.

8.9 Article 21 – Right to Object

The right to object to processing is not relevant for CCR and direct care. Objection to processing is largely based on the performance of a task in the public interest, the legitimate interests of the data controller (Articles 6 (e), (f)) and to prevent direct marketing.

How the CCR complies with this requirement

As Article 6 (e) and 6 (f) are not legal bases used by the CCR programme and there is no direct marketing element to the processing of patient and service user data, then this right is not relevant for CCR.

8.10 Article 22 - Automated individual decision-making, including profiling

Individuals have a right not be subject to decision based solely on automated processing which produces legal affects concerning them or similarly significantly affects them.

How the CCR complies with this requirement

No automated decision-making takes place under CCR. This right is not relevant in this context.

Recommendation 14: Rights of the Data Subject (Risk 13 – DPIA)

The rights of the data subject have been redefined and made strong under GDPR. It is important that data controllers are aware of their existing and new obligations and that systems have audit trails to log activity.

The CCR Governance Group are recommended to ask partners to reassure them that training is in place, and that the right of individuals will be upheld, that consent and dissent will be respected and acted upon and that individual's will be supported with questions they may have.

RISK 14: HIGH

Risks are ever present where the rights of individuals are concerned and failure to act correctly can be interpreted as obstruction to those rights. It is therefore essential that risks to individual's rights are noted and actively managed with mitigations in terms of training, systems operation and support brought in where possible, particularly via IG Governance Group receiving partner assurances.

Failure to comply with individuals' rights is potentially the highest risk carried by the CCR as it brings with it the issues of ICO actions, individual complaint and action, compensation and fines.

9 Conclusion

This DPIA has been redrafted using the originally published document and modifying it to ensure that changes to data protection laws since the publication are now reflected.

The changes in the law present an opportunity for the governance group to reengage with the programme, to ensure that risks are appropriately managed and that suitable changes are made to processes which may no longer be fit for purpose under new GDPR, DPA 2018 rules.

Each organisation should keep a record of this document, and any future iterations, and have them approved by the relevant committee, group or individual in that organisation, prior to taking part in the CCR.

All recommendations made should be considered, implemented, and recorded as complete by the individual organisations Information Governance Group (IGG) and signed off by the Caldicott Guardian, who should have reviewed the approach to the use of the system to ensure patient rights are protected.

Partner Organisations should have regard particularly to the Fair Processing or Privacy Notices and publish updates to their own as necessary, including ensuring the information is accessible to the whole population, in addition to the wider CCR communications campaign.

10 Appendix 1 – Version History and Table of Amendments

Version History

Version	Date issued	Updated by	Reason
0.1	5th March 2014	David Birkinshaw	First Draft
0.2	17th June 2014	David Birkinshaw	Second Draft
0.3	6th July 2014	David Stone	Final Draft
1.0	20th July 2014	David Stone	Final
1.1	24th Sept 2014	Jackie Millar	Reviewed by WCCR Governing Group
1.2	6th Oct 2014	Jackie Millar	Signature page added
2.0	13 May 2015	David Stone	New iteration to reflect expansion of WCCR to CCR and the new risk environment
2.01 DRAFT	29th June 2018	Simon Howarth	Rewritten, following review to bring DPIA up to date with new legislation (GDPR) and to review risks and recommendation in the new context.
2.02 DRAFT	1st July 2018	Simon Howarth	Additions around consenting, further review of risk scores.
V3.0 FINAL	January 2019	Simon Howarth	Reviewed in light of CCR Governing Group member comments.

11 Appendix 2 – Recommendations & Risks

Title	Recommendation	Risk Desc.	Risk Likelihood x Consequence	Risk Score	CCR / Partner Response.
1: Communication of information risks and CCR Governing Group	a. The CCR Governing group should be reviewed for attendance, reformed and formal dates set with standing agendas and a review of the terms of reference. b. The group should be tasked with reviewing risks, assessing the risk scoring and each partner organisation including relevant risk into their information risks registers. c. The CCR Governing Group should consider the risks identified, approve the mitigating controls and determine whether the residual risk level is acceptable. Where the remaining risk is unacceptable, the CCR Governing Group should agree what further risk-mitigating controls are required and implement a mechanism to ensure these are put in place	Governance of the programme is required and decision making, security and confidentiality must be a priority to provide assurances to the group members and, if necessary, assurances to the wider public and the regulator. There is a risk that the group not meeting properly in a structured manner means that any breach may not be handled properly and lead to serious criticism and reputational loss, along with potential higher fines.	3 x 5 = 15	HIGH	
2: Contracts and agreements review	Contracts and sharing agreements between all involved parties should be reviewed and updated to reflect new legislative requirements.	Contracts that are no longer fit for purpose represent a risk in that parts of the documents may be no longer reliable in the case of a dispute. In the case of a data processor contract being invalidated, this defaults the processor to a data controller. Risks related to a failure based on contractual requirements can be mitigated, largely by a formal	3 x 4 = 12	MEDIUM HIGH	

Title	Recommendation	Risk Desc.	Risk Likelihood x Consequence	Risk Score	CCR / Partner Response.
		review and where necessary new or amended contracts and agreements.			
3: Management of data flows	The management of data flows is important as it relates directly to the Records of Processing requirements, providing a basis for managing flows and understanding what categories of data etc., are being processed. A tool to help manage this process is recommended, so that changes to processing flows and types can be reflected swiftly and with lower management resource impact. Regardless of whether a tool is used, the records of processing must be in a reasonable state as it may be requested by the ICO at any time. Failure to supply such information in a timely manner will at best bring criticism and at worse cause action to be taken against data controllers. All controllers must themselves create and manage a records of processing. A consistent approach to this will make creation of a CCR flows/map easier.	A lack of good records of processing information and data mapping leaves organisations open to criticism and more punitive action, in the event of a data breach. Understanding the information flowing through systems and organisations is a fundamental part of information management.	3 x 4 = 12	MEDIUM HIGH	
4: Future need for closer integration	It should be recognised that, as integrated health and social care matures, future uses of the CCR system may require coordinated care plans to which multiple providers contribute. The CCR Governing Group will	The ability of the CCR Governance Group to assess and review potential helpful changes and decide on how the CCR, if at all, can be used is important to the future	3 x 2 = 6	MEDIUM LOW	

Title	Recommendation	Risk Desc.	Risk Likelihood x Consequence	Risk Score	CCR / Partner Response.
	need to commission an in-depth review of the agreement/contract and PIA should this eventuality arise as it may require a considerable change. Such a change would require extensive stakeholder engagement and a reconsideration of any existing consent.	development and use of the CCR. Not building such processes into the Governance Group risks the system becoming less effective in areas of growth in the health sector.			
5: Patient Objection Management Systems	All Partner Organisations should re-confirm they have internal systems and have trained their staff to respond to questions from patients arising from the public communications to take action where a patient expresses their wish to dissent from the sharing of their personal data.	Partner organisations without the ability to control consent and dissent, and thereby stop the sharing of patient data at the patient's request risk complaints and investigation by the ICO as to the management of patient data. However, it is recognised that legacy systems are difficult to amend and change and in the current climate of tight resources this risk may need to be accepted and the possibility it brings to shining a light on the CCR and how it handles data, should complaints become an issue.	3 x 5 = 15	HIGH	
6: Review of existing basis for implying consent to share	Review of existing patient information should be repeated to ensure inclusion of GDPR references and changes to individuals rights and freedoms along with references to outside, valid guidance.	It is important that communications and fair processing is kept up to date to manage risks related to patients failing to be adequately informed, and subsequent investigation by the ICO leading to criticism and the potential loss of trust in the system.	4 x 4 = 16	HIGH	

Title	Recommendation	Risk Desc.	Risk Likelihood x Consequence	Risk Score	CCR / Partner Response.
7: Review Communications to hard to reach groups	Ensure that the materials and communication channels are still in effect, to reach the entire population to support implied consent with consideration for a further equality and diversity assessment to ensure that effective communications reaches the more hard to reach groups.	Assuming that action was taken at the launch of the CCR to include hard to reach groups, then this review will help to mitigate a medium-low risk that these channels are not still operating and that it may lead to complaints.	4 x 4 = 16	HIGH	
8: Partner Organisations review their ICO registration and include any new purposes	Review the purposes and make suitable changes in light of the GDPR changes where there may be a change in data processed. This will help as evidence of due diligence for each data controller.	It is understood that all partners have registrations in place and that a review would promote good practice. There is little risk if this is not carried out, but could potentially lead to the ICO requiring a registration to be updated if thought to be inaccurate or out-of-date.	1 x 2 = 2	LOW	
9: Confirm that training for Health and Social Care professionals in IG is up to data and that they are informed of the CCR and its uses including the management of data flows	Reconfirm that each partner organisation is continuing to ensure staff are adequately trained and that health and social care professionals using the CCR have training to identify and manage data flows so that they can review these flows regularly.	This risk is linked to Recommendation 3 as it is important in the context of training that data flows are managed and recorded effectively. Health and social care professionals using a tool to manage the data flows will be able to review theirs and others to ensure no conflicts. Failure to do this risks data flows not being managed properly and data transferring to place it may not be sanctioned for.	2 x 3 = 6	MEDIUM LOW	
10: Data Quality procedures	The CCR Governing Group should establish, or re-engage, a sub-group to either coordinate Partner Organisation reporting	Clinical inaccuracies, or differences may lead to individuals' being treated with information that is not	3 x 5 = 15	HIGH	

Title	Recommendation	Risk Desc.	Risk Likelihood x Consequence	Risk Score	CCR / Partner Response.
	of discrepancies in the data, or design processes for adoption by all Partners to address data quality issues. These are inevitable and could be a clinical risk if the differences are not understood. Whatever strategy is adopted, it must consider training for staff in how to respond to seeing discrepancies in the record.	fit for purpose and may delay or complicate treatment or potentially ultimately cause death.			
11: Storage in CCR system	The use of Graphnet hosted on a local system at Countess of Chester Hospital (COCH), brings with it some risks in terms of ensuring continued security and confidentiality and long term access to the system should the Hospital cease, or pull out of the CCR. A review of the appropriateness of local storage and the agreements in place is recommended. A review of retention and storage policies and processes should be undertaken, with any concerns of changes being reflected in planned modifications to ensure the continued good working of the systems.	With local storage it is important that security set up and confidentiality are maintained to manage the risks related to information being available locally where it shouldn't be and to manage potential intrusions into the hosting systems.	3 x 4 = 12	MEDIUM HIGH	
12: IT Security Review	Locally held systems will need to have assurances and evidence that IT security is of a standard acceptable to the CCR Governing Group and that there is compliance with required standards.	There is always a risk related to IT security and unauthorised accesses to systems. This risk can be reduced through the application of good testing and reporting of the standards used to secure the	3 x 5 = 15	HIGH	

Title	Recommendation	Risk Desc.	Risk Likelihood x Consequence	Risk Score	CCR / Partner Response.
	A penetration test and report on the IT Security of the Graphnet system and the data flows will ensure that the security remains fit for purpose.	system and clarification that the system is as robust as possible.			
13: Access controls and user profiles	All organisations should review their procedures and ensure that a member of staff is allocated as the system administrator, and take part in appropriate training in order to ensure that appropriate user profiles are allocated. Similarly, procedures must be in place to ensure users are removed from the system access if they no longer have legitimate access. Role based access schedules need to be in place to ensure that only those people with legitimate business need can access what they require to do their roles.	Access to systems must be controlled with authorised staff only being allowed access to the system. They must be managed in a way that ensures they are added correctly and removed when the time comes and their access is commensurate with the role they perform. Failure to manage this process properly risks access by individuals who have no rights to be there and a potential breach of confidentiality and security which in turn may be reportable as a data breach to the ICO.	3 x 4 = 12	MEDIUM HIGH	
14: Rights of the Data Subject	The rights of the data subject have been redefined and made strong under GDPR. It is important that data controllers are aware of their existing and new obligations and that systems have audit trails to log activity. The CCR Governance Group are recommended to ask partners to reassure them that training is in place, and that the right of individuals will be upheld, that consent and dissent will be respected and acted upon and that individual's will be supported with questions they may have.	Risks are ever present where the rights of individuals are concerned and failure to act correctly can be interpreted as obstruction to those rights. It is therefore essential that risks to individual's rights are noted and actively managed with mitigations in terms of training, systems operation and support brought in where possible, particularly via IG Governance Group receiving partner assurances.	4 x 5 = 20	HIGH	

Title	Recommendation	Risk Desc.	Risk Likelihood x Consequence	Risk Score	CCR / Partner Response.
		Failure to comply with individuals' rights is potentially the highest risk carried by the CCR as it brings with it the issues of ICO actions, individual complaint and action, compensation and fines.			

12 Appendix 3 – Reference documents

12.1 Data to be processed

The following is a summarised list of information contained in the flows, taken from the detailed dataset in the system. Note that contractually between each Data Controller and the Data Processor, this will be bound in contract as the only data which are to be processed.

Hub Data Guide V0 15 clean.docx

12.2 Information for General Practice staff

A guidance pack that practices can use to inform their staff as to the rights of patients in this CCR, and their right to opt out of sharing their data if they wish. Under review as part of the wider review of activities, post GDPR implementation.

GP Practice Guidance v0.1.doc

12.3 CCR Privacy Notice

Recommended text for all organisations. Under review as part of the wider review of activities, post GDPR implementation.

Fair Processing Notice.docx

12.4 CCR patient information leaflet recommended text

Recommended text for patient information leaflet to be made readily available to patients at all organisations taking part in the CCR and which is in use currently. This is under review as part of the wider review of activities, post GDPR implementation.

CCR draft patient leaflet text .docx

12.5 READ Codes to be used to record dissent

The following READ Codes should be used to ensure individuals' wishes not share their data is recorded and the system no longer uploads their data:

Graphnet System Opt Out process.docx