Data Processing Agreement

between

Signatory Controllers

and

Countess of Chester Hospital NHS Foundation Trust (Processor)

Version: 4.0 FINAL
Issued: 14th May 2019

Summary

Title:	Data Processing Agreement between Signatory Controllers and Countess of Chester Hospital NHS Foundation Trust ("CoCH") (Processor)
Purpose:	The signatories to this Agreement have agreed to contract Countess of Chester Hospital NHS Foundation Trust (Processor) as a Processor for the purpose of management of approved sub-processor contracts for the supply of systems and services. This Agreement regulates the processing of Personal Confidential Data (PCD) by CoCH and its sub-processors on behalf of the Signatories. This Data Processing Agreement is a contract which sets out the binding terms for processing PCD, including the subject-matter and duration of the processing; the nature and purpose of the processing; the type of personal data and categories of data subjects; safeguards and security measures; and the obligations and rights of the respective parties.
Signatories:	Signatories are recorded in schedule 7
Commencement date:	14th May 2019
Review date:	14th May 2021
Agreement owner:	Data Protection Officer – Countess of Chester Hospitals NHS Foundation Trust.

TABLE OF AMENDMENTS

Version	Clauses Amended	Date	Summary of Amendments
1.1	Multiple	19-Jul-2018	Amendments to processor obligations, general amendments for CCR use (draft)
2.0	Multiple	Jan-2019	Final review following comments and reference to changes in protocol and DSA.
3.0	Multiple	April 2019	Updated to stream line the need for several documents.
4.0	Multiple	May 2019	Updated to incorporate changes follow CCR Governance Meeting 13/05/19. FINAL VERSION

Contents

1 Recitals

(A) The DPA meets the requirements of the General Data Protection Regulation 2016/679 (GDPR) and Data Protection Act 2018 which established the duty of controllers to bind processors in contract to act only on the controller's instructions and to provide guarantees to ensure that the processing of the data carried out on its behalf is secure and appropriate.

(B) This DPA sets out the specific details of the data processing in respect of the Cheshire Care Record (CCR).

(C) Operation of this Agreement is governed by the CCR Information Governing Group to which all schedule signatories are a member by virtue of being a signatory to this DPA. The CCR Information Governance Committee operates in accordance with its Terms of Reference.

(D) Schedule Signatories (Signatories) have agreed to establish the CCR data set to support integrated care design and delivery and other purposes permitted this DPA.

(E) Signatories will only share PCD necessary for the permitted purposes of the CCR unless an individual objects in accordance with their rights in the DPA.

(F) The CCR data set includes Personal and Special Categories of coded PCD extracted from Signatory records. Some data codes are excluded (see Schedule 2: Data inclusions and exclusions).

(G) Personal and Special Categories of data are processed only in accordance with permitted uses in this DPA.

(H) CCR systems provide Signatories with data analytical services, with appropriate access right controls, including analysis to support identification of people who may benefit from targeted care (Risk Stratification for Case Finding), and a website for public communications and transparency.

(I) This DPA does not provide for any Clinical Commissioning Groups which are Signatories to have any access to PCD. This would be a breach of the Common Law Duty of Confidentiality.

(J) All data must be minimised and de-identified at every opportunity in accordance with applicable law and guidance. Evidence of this effort should be documented in the Data Protection Impact Assessment (DPIA).

(K) It is the responsibility of the CCR Information Governance Committee to complete and maintain a review of a Data Protection Impact Assessment in accordance with GDPR article 35.

(L) Signatories must provide contact details for the person accountable for this DPA and their Caldicott Guardian, Senior Information Risk Owner and Data Protection Officer. This contact information must be entered and maintained in the CCR Governance Contact Information held by the CCR System Administrator and regularly reviewed by the CCR Information Governance Group.

2 Data Processing Agreement

THIS DATA PROCESSING AGREEMENT is made on 14th May 2019 BETWEEN:

(1) The Signatories listed in Schedule 7; and

(2) CoCH incorporated in, or existing and established under the laws of the UK whose registered office is at Countess of Chester Health Park, Liverpool Road, Chester, CH2 1UL (Processor).

1 Permitted purposes of processing

1.1 Personal Confidential Data (PCD) may be processed for the specified purposes of the Data Sharing Protocol, as amended from time to time, to the extent it is necessary to deliver a service instructed by the CCR Information Governance Committee. Specified purposes for this schedule are:

1.1.1 Health and Social Care (GDPR Article 9(2)(h))
1.1.2 Public Health (GDPR Article 9(2)(i))
1.1.3 Archiving, Scientific Research and Statistics (GDPR Article 9(2)(j))
1.1.4 Database Maintenance (GDPR Article 6(1)(b)

1.2 PCD may only be accessed and shared to the extent permitted by applicable law and in a manner compatible with the rights and freedoms of the individual, NHS Constitutional rights and Caldicott Guardian Principles.

1.3 Where PCD may be processed exceptionally for the purpose of database management and repair, access must be logged by the Processor or sub-processor and reported to the CCR Information Governance Committee.

1.4 The Processor may be instructed to de-identify data by the CCR Information Governance Committee and to allow access to such data under sub-contracts operated by the Processor according to rules and reporting requirements approved by the CCR Information Governance Committee.

2 Benefits

2.1 The benefits of data processed under this schedule are expected to be:

2.1.1 better access for care professionals to a patient's health and social care history for individual care planning;
2.1.2 more integrated planning and working between care professionals; and
2.1.3 better understanding for care professionals of conditions shared by their own patients and clients.

2.2 The Signatories agree that shared information will be de-identified in accordance with all applicable law and guidance so that it may be used for the approved purpose of the CCR Information Governance Group.

2.3 In particular, access to a de-identified version of the CCR data (the CCR De-identified Dataset) will be used by Signatories to provide for information and analysis without the need for identifiers.

2.4 All parties recognise that 'consent' arrangements are needed in respect of sharing information to comply with the Common Law Duty of Confidentiality. This is not to be confused with the types of consent necessary to satisfy privacy legislation.

3 Common law duty of confidentiality

3.1 In order to satisfy the Common Law Duty of Confidentiality as it relates to the processing purposes under this schedule, each Signatory shall:

3.1.1 effectively inform patients about the ways in which the data they have provided may be used, who it may be shared with, what is shared and for what purpose;

3.1.2 effectively inform patients where they have the right to opt-out of sharing their data or select/restrict which elements of their data may or may not be shared and that any consent can be changed in the future;

3.1.3 in accordance with the NHS Constitution, where a patient's objections cannot be followed, to effectively inform the patient of the reasons why;

3.1.4 effectively inform patients of the implications for the provision of care or treatment, such as the potential risks involved if their full Individual Integrated Care Record is not made available to health professionals involved in their care;

3.1.5 ensure privacy notices are delivered in accordance with the ICO Privacy Notice Code of Practice;

3.1.6 employ a variety of channels relevant to the service delivery model to communicate with people regarding data sharing, such as information leaflets and posters at the point of care, during the patient registration process, appointment letters, or when referring into other services.

3.2 Signatories must have a mechanism in place to deal with patients' requests to have their records excluded from the data sharing where they may be identified, either by excluding such records from their data extracts or by flagging them so that the systems do not allow those records to be viewed. This must allow patients to opt back in and for the marker to be removed.

3.3 Consent to satisfy the Common Law Duty of Confidentiality need not be sought for use of the CCR De-identified Dataset for commissioning purposes, as no PCD shall be used. This does not alter the communication duties described above as processing for this purpose must still be transparent.

4 Legal basis for processing

4.1 Each Provider Signatory agrees that it is a Controller in respect of Personal Data that it discloses and a Joint Controller in respect of any information that it accesses from CCR systems.

4.2 CoCH agrees that it is a Processor in respect of data processed under this DPA and is authorised only to act on the written instructions of the Controllers.

4.3 All parties shall comply at all times with all applicable Laws and regulations relating to processing of personal data and privacy in effect in England and Wales including where applicable the guidance and codes of practice issued by the Information Commissioner, the Department of Health, General Medical Council and other relevant regulators and shall not perform its obligations under this DPA in such a way as to cause any other party to this DPA to breach any of its obligations under such applicable Laws, regulations or guidance.

4.4 Signatories accessing the CCR De-identified Dataset (and any contractors acting on their behalf) are obliged by contract not to seek to further link and or re-identify data in the CCR De-identified Dataset, including not to use the data to identify any individual or make any decisions relating to any individual.

5 Data management and access requests

5.1 Signatories are accountable for the accuracy, completeness and validity of the PCD shared and that appropriate security and confidentiality procedures are in place to protect the transfer and use of the shared PCD.

5.2 The Processor is required to create and maintain, in relation to processing carried out under this DPA:

5.2.1 an information asset register that also satisfies GDPR article 30 or Schedule 1, Part 4, Para 1, Data Protection Act 2018;

5.2.2 data flow maps that identify each exchange of data, the lawful basis and any data transformation; and

5.2.3 Reporting on data quality to the CCR Information Governance Committee

5.2.4 risk registers, identifying risks including contract, quality and processing.

5.3 Each Signatory is a Controller and is responsible for handling subject access requests made under Article 15 of the GDPR. Each Signatory shall assist others in responding to requests or other exercising of rights made under Data Protection Legislation, in accordance with the Protocol.

5.4 The Signatories instruct that a subject access request made to CoCH shall be satisfied by them in respect of CCR data. The Processor is required to establish a system, for the approval of the CCR Information Governance Committee, that complies with the requirements of the privacy legislation.

6 Information governance and data security

6.1 Signatories are accountable for the information governance and security of the PCD shared including the operation of appropriate technical and organisational controls in accordance with the DPA.

7 Access to data

7.1 Signatories must strictly restrict access to CCR data to only those staff that have an essential need and in accordance with the terms of the Protocol and this schedule.

7.2 The Processor must establish and operate procedures and reporting such that only authorised persons accessing CCR systems have access by secure logins and associated audit trails. For all accesses of PCD the audit trail will identify the at least the following information:

7.2.1 Job role and name of staff member accessing the system;
7.2.2 Organisation name;
7.2.3 What actions were performed; and
7.2.4 The date and time the information was viewed.

7.3 Signatories that become aware of a Security Incident shall immediately inform the CCR Information Governance Committee (by email to: cochservice.desk@nhs.net) and all affected Signatories with as many details as known at that time. Any affected Signatory shall investigate the Security Incident using their data loss or data breach procedures. Affected Signatories will report to the CCR Information Governance Committee thereafter, including the findings of any subsequent investigation report or remedial actions.

7.4 The Processor will maintain a log of reported security incidents for each schedule under the Protocol and publish this on request.

8 Method for sharing data

8.1 Data transfers will be made in accordance with Secure File Transfer Protocols within the N3 network and/or in accordance with NHS Digital's Good Practice Guidelines.

9 Data retention

9.1 An initial data upload is extracted and processed for inclusion in the CCR data set as soon as possible after a new organisation signs their agreement and is approved by the CCR Information Governance Committee.

9.2 Subsequent changes to that data are replaced through real time or subsequent data feeds.

9.3 If a patient later opts out, the Signatory will flag their record for exclusion and the data will be purged as soon as is reasonably possible.

9.4 If a Signatory ceases to participate in the CCR, no further data is extracted, and the remaining Signatories remain Joint Data Controllers for the data.

9.5 Data that is created in CCR, including audit trails, access logs, etc., should be retained in accordance with the NHS Records Management Code of Practice for Health and Social Care. Relevant retention will be noted against assets in the Information Asset Register

10 De-identification data

10.1 Signatories may access the CCR De-identified Dataset, provided that they shall not:

10.1.1 attempt to re-identify any data contained within the CCR De-identified Dataset;

10.1.2 use any data contained within the CCR De-identified Dataset to identify any individual;

10.1.3 use any data contained within the CCR De-identified Dataset to take a decision about any specified individual or individuals;

10.1.4 attempt to link data in the CCR De-identified Dataset with any other dataset; or,

10.1.5 share data contained within the CCR De-identified Dataset with any third party, apart from where contracted as a processor subject to contractual terms no less onerous than those imposed by this DPA.

10.2 Signatories may only use or allow to be used data from the CCR De-identified Dataset in connection with the statutory functions of or connection with their statutory functions as a provider or commissioner of health and/or social care or provider of public health.

11 Obligations of the Processor

11.1 The Parties acknowledge that for the purposes of the Data Protection Legislation, the Provider Signatories are the Controllers and CoCH is the Processor.

11.2 The Processor is instructed to only process data under this agreement in accordance with the written instructions contained herein, subsequent written instructions of the CCR Information Governance Committee.

11.3 The Processor shall provide the Controllers with whatever information it reasonably needs to ensure the Controller and the Processor, and any Sub-processor are meeting their respective obligations under the EU General Data Protection Regulation (GDPR) and Data Protection Act 2018.

11.4 The Processor shall notify the Controllers immediately if it considers that any of the Controller's instructions infringe the Data Protection Legislation.

11.5 The Processor shall provide all reasonable assistance to the Controller in the preparation of any Data Protection Impact Assessment prior to commencing any Processing. Such assistance may, at the discretion of the Controller, include:

11.5.1 a systematic description of the envisaged Processing operations and the purpose of the Processing;

11.5.2 an assessment of the necessity and proportionality of the Processing operations in relation to the Services;

11.5.3 an assessment of the risks to the rights and freedoms of Data Subjects;

11.5.4 the measures envisaged necessary to address the risks, including safeguards, security measures and mechanisms to ensure the protection of Personal Data; and

11.5.5 assisting the Controller in meeting its obligation to consult with the Supervisory Authority where a Data Protection Impact Assessment indicates the Processing would result in an unmitigated high risk.

11.6 The Processor shall, in relation to any PCD processed in connection with its obligations under this Contract:

11.6.1 process that PCD only in accordance with this DPA unless the Processor is required to do otherwise by Law. If it is so required, the Processor shall promptly notify the Controllers before processing the PCD unless prohibited by Law;

11.6.2 maintain appropriate confidentiality, information security, data protection and records management policies, copies of which shall be provided to the Controllers on request;

11.6.3 comply with any additional polices or procedures as required by the Signatories acting as Joint Controllers;

11.6.4 ensure that it has in place Protective Measures, which have been reviewed and approved by the Controller as appropriate to protect against a Data Loss Event having taken account of the:

11.6.4.1 nature of the data to be protected;

11.6.4.2 harm that might result from a Data Loss Event;

11.6.4.3 state of technological development; and

11.6.4.4 cost of implementing any measures.

11.6.5 ensure that it complies with the National Data Guardian 10 Security standards;

11.6.6 ensure that it complies with security standards as set out in the Data Security and Protection Toolkit;

11.6.7 ensure that it adheres to relevant legal and professional requirements, in particular in relation to data protection, human rights and common law obligations such as the duties of care and confidentiality ensure that:

11.6.7.1 the Processor staff do not process PCD except in accordance with this Contract (and in particular clause 1 of this DPA);

11.6.7.2 it takes all reasonable steps to ensure the reliability and integrity of any staff who have access to the PCD and ensure that they:

11.6.7.2.1 are aware of and comply with the Processor's duties under this DPA;

11.6.7.2.2 are subject to appropriate confidentiality undertakings with the Processor or any Sub-processor;

11.6.7.2.3 are informed of the confidential nature of the PCD and do not publish, disclose or divulge any of the Personal Data to any third party unless directed in writing to do so by the Controller or as otherwise permitted by this Contract; and

11.6.7.2.4 have undergone adequate training in the use, care, protection and handling of PCD.

11.7 The CCR Information Governance Committee and the data processor will agree actions required if the organisation is taken over, goes out of business or is in administration:

11.7.1 The data processor develops an exit strategy in relation to the processing of data under this DPA. This includes returning the data the data controllers and/or secure destruction of the data upon instruction from the CCR Information Governance Committee.

11.8 The Processor shall notify the Controllers immediately if it:

11.8.1 receives a Data Subject Access Request (or purported Data Subject Access Request);

11.8.2 receives a request to rectify, block or erase any PCD;

11.8.3 receives any other request, complaint or communication relating to either Party's obligations under the Data Protection Legislation;

11.8.4 receives any communication from the Information Commissioner or any other regulatory authority in connection with Personal Data Processed under this Contract;

11.8.5 receives a request from any third party for disclosure of PCD where compliance with such request is required or purported to be required by Law; or

11.8.6 becomes aware of a Data Loss Event.

11.9 The Processor's obligation to notify under clause 11.8.6 of this DPA is restricted to reporting details of the breach only to the controllers and to no other entity unless required to do so by the Information Commissioner.

11.10 The Processor's obligation to notify under clause 11.8 of this DPA shall include the provision of further information to the Controllers in phases, as details become available.

11.11 Taking into account the nature of the Processing, the Processor shall provide the Controller with full assistance in relation to either Party's obligations under Data Protection Legislation and any complaint, communication or request made under clause 11.8 of this DPA (and insofar as possible within the timescales reasonably required by the Controllers) including by promptly providing:

11.11.1 the Controller with full details and copies of the complaint, communication or request;

11.11.2 such assistance as is reasonably requested by the Controllers to enable the Controller to comply with a Data Subject Access Request within the relevant timescales set out in the Data Protection Legislation;

11.11.3 the Controllers, at its request, with any PCD it holds in relation to a Data Subject;

11.11.4 assistance as requested by the Controllers following any Data Loss Event;

11.11.5 assistance as requested by the Controllers with respect to any request from the Information Commissioner's Office, or any consultation by the Controllers with the Information Commissioner's Office.

11.12 The Processor shall maintain complete and accurate records and information in writing or electronic form to demonstrate its compliance with this DPA.

11.13 Records of processing activities must include:

11.13.1 the name and contact details of the processor or processors and of each controller on behalf of which the Processor is acting, and, where applicable, of the controller's or the processor's representative, and their Data Protection Officer;

11.13.2 the categories of processing carried out on behalf of each controller;

11.13.3 a general description of the technical and organisational security measures referred to in Article 32(1) of the GDPR.

11.13.4 Reflect detail specified within the Policy Document and whether the personal data is retained and erased in accordance with the policies and, if it is not, the reasons for not following those policies.

11.14 The Processor shall allow audits of its Processing activity by the Controller or the Controller's designated auditor.

11.15 The Processor shall designate a Data Protection Officer and publish details on its website.

11.16 The Processor shall provide details for significant persons and contacts for day to day management of the service or provision on the Information Sharing Gateway.

11.17 The Processor shall maintain registration with the Information Commissioner under provisions set out under the Digital Economy Act 2017..

11.18 The Controllers may, at any time on not less than 30 Business Days' notice, revise this DPA by replacing it with any applicable controller to processor standard clauses or similar terms forming part of an applicable certification scheme (which shall apply when incorporated by attachment to this Contract).

11.19 The Parties agree to take account of any guidance issued by the Information Commissioner's Office. The Controller may on not less than 30 Business Days' notice to the Processor amend this DPA to ensure that it complies with any guidance issued by the Information Commissioner's Office.

11.20 The Processor shall comply with any further instructions with respect to Processing issued by the Controller by written notice. Any such further written instructions shall be deemed to be incorporated into this DPA from the date at which such notice is treated as having been received by the Processor.

11.21 The Processor will maintain a Policy Document and operating manual, updated by written instruction of the CCR Information Governance Committee and which incorporates the terms of this agreement which apply to its operation, and historic instructions.

11.22 The Policy Document will record how the processing meets the Article 5 principles, retention schedules and erasure process and must be reviewed on a regular basis. If updated, the Processor is required to update the records of processing. The policy document is to be retained for six months after the destruction of the data.

11.23 Any change or other variation to this DPA shall only be binding once it has been agreed in writing and signed by an authorised representative of both Parties.

12 Specific obligations of the Processor

12.1 The Processor and sub-processors, to the extent required by the terms and conditions of sub-processing contract (but otherwise the following shall not apply to sub-processors), shall:

12.1.1 Enter into, manage and enforce the provisions of contracts necessary to deliver the Purposes.

12.1.2 Provide technical and other support to service this Agreement and support the CCR Information Governance Committee.

12.1.3 Provide implementation and set-up assistance for CCR .

12.1.4 Transfer only approved data from Provider Signatories and NHS Digital into the CCR systems as approved from time to time by the CCR Information Governance Committee.

12.1.5 Maintain CCR systems, including by human intervention where required to ensure data integrity.

12.2 Comply with the obligations imposed on it by this DPA as a data processor, and specifically shall (and shall, unless specifically approved by the CCR Information Governance Committee to enter into specific arrangements on different terms with any sub-contractor or sub-processor, shall ensure that any sub-contractors processing personal data shall):

12.2.1 process the PCD only in accordance with instructions from the CCR Information Governance Committee, which may be specific instructions or instructions of a general nature as set out in this DPA or as otherwise notified by the CCR Information Governance Committee to the Processor during the term of this DPA;

12.2.2 process the PCD only to the extent, and in such manner, as is necessary for the purposes of this DPA or as is required by law or any regulatory body. For the avoidance of doubt this shall include;

12.2.2.1 addressing data quality issues in the data feeds;

12.2.2.2 supporting system developments;

12.2.2.3 de-identifying data for the CCR De-identified Dataset.

12.2.3 take reasonable steps to ensure the reliability of any of staff who have access to the personal data;

12.2.4 implement appropriate technical and organisational measures to protect the personal data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure. These measures shall be appropriate to the harm which might result from any unauthorised or unlawful processing, accidental loss, destruction or damage to the personal data and having regard to the nature of the personal data which is to be protected;

12.2.5 obtain prior written consent from the CCR Information Governance Committee before transferring any personal data to any sub-contractors or any other third party;

12.2.6 ensure that all the Processor's staff required to access the personal data are informed of the confidential nature of the personal data and are contractually obliged and trained to comply with the obligations set out in this DPA;

12.2.7 ensure that none of the Processors staff publish, disclose or divulge any of the personal data to any third party unless directed in writing to do so by the CCR Information Governance Committee;

12.2.8 notify the CCR Information Governance Committee within five working days if it receives:

12.2.8.1 a request from a data subject to have access to that person's personal data; or

12.2.8.2 a complaint or request relating to the Processor's obligations as such under the Data Protection Legislation.

12.2.9 provide the CCR Information Governance Committee and any Signatory with full cooperation and assistance in relation to any complaint or request made, including by:

12.2.9.1 providing full details of the complaint or request;

12.2.9.2 complying with a data access request within the relevant timescales set out in the Data Protection Legislation and in accordance with the CCR Information Governance Committee or relevant Provider Signatory's reasonable instructions;

12.2.9.3 providing the CCR Information Governance Committee or relevant Provider Signatory with any personal data it holds in relation to a data subject (within the timescales reasonably required by the CCR Information Governance Committee or relevant Provider Signatory); and

12.2.9.4 providing the CCR Information Governance Committee or relevant Provider Signatory with any information reasonably requested by the CCR Information Governance Committee or relevant Provider Signatory;

12.2.10 permit the CCR Information Governance Committee (subject to reasonable and appropriate confidentiality undertakings), to inspect and audit the Processor's data processing activities and comply with all reasonable requests or directions by the CCR Information Governance Committee to enable the CCR Information Governance Committee to verify and/or procure that the Processor is in full compliance with its obligations as such under this DPA;

12.2.11 provide a written description of the technical and organisational methods employed for processing personal data (within the timescales reasonably required by the CCR Information Governance Committee); and

12.2.12 not transfer any personal data outside England without written instruction of the CCR Information Governance Committee.

12.2.13 not make further copies of personal data, except for back-up copies as necessary, and except where de-identified in accordance with instructions of the CCR Information Governance Committee.

12.2.14 Carry out its obligations under this DPA in compliance with Data Protection Legislation.

12.3 Afford shared data the highest appropriate industry standard secure storage including ensuring that hardware utilised for the purposes of this DPA is kept in a physically secure environment protected by a fully managed industry standard firewall.

12.4 Use, and ensure that the latest versions of anti-virus definitions and software available from an industry accepted anti-virus software vendor are used to check for, contain the spread of, and minimise the impact of malicious software.

12.5 Maintain and implement a business continuity and disaster recovery plan to the reasonable satisfaction of the CCR Information Governance Committee.

12.6 Arrange for independent audits of the security and resilience of the software and physical and virtual systems, networks and hardware (including the non-technical management and organisational processes necessary to limit the accessibility of the virtual environment) in conjunction with the CCR Information Governance Committee.

12.7 Backup servers to the extent necessary to maintain the service and retain audit trails.

12.8 Ensure that on the expiry or termination of this DPA, the PCD held by the Processor or its sub-processors is destroyed in accordance with the then current NCSC standard for the level of data sensitivity, and is migrated to an alternative software provider if required.

12.9 Produce and keep up-to-date the CCR De-identified Dataset, which shall be a copy or view of the CCR dataset, de-identified to a standard determined by the CCR Information Governance Committee from time to time and recorded in the operating manual.

13 Processor service charges and charging arrangements

13.1 The Signatories shall ensure that the Processor is remunerated for its services in accordance with the principles set out in schedule 6.

14 Sub-processing

14.1 The Processor may not sub-contract any of its obligations without the prior written consent of the CCR Information Governance Committee. The CCR Information Governance Committee may authorise the Processor to contract a third party or third parties (each, Sub-Processor) to:

14.1.1 process PCD on behalf of the Signatories; and/or

14.1.2 carry out any of the Processor's other obligations under this DPA.

14.2 Before allowing any Sub-Processor to process PCD under this Contract, the Processor must:

14.2.1 notify the CCR Information Governance Committee in writing of the proposed Sub-Processor and processing activity;

14.2.2 obtain the written instruction of the CCR Information Governance Committee;

14.2.3 enter into a written DPA with the Sub-Processor which give effect to the terms set out in this DPA, Information Governance Requirements and Due Diligence for Sub-processors, such that they apply to the Sub-processor; and

14.2.4 provide the CCR Information Governance Committee with such information regarding the Sub-processor as the CCR Information Governance Committee may reasonably require.

14.3 The Processor shall remain fully liable for all acts or omissions of any Sub-Processor.

14.4 The Processor is authorised to appoint the following Sub-Processors to process PCD on behalf of the Signatories:

14.4.1 Softcat Limited, Morton House, Thames Valley Ind. Park, Marlow, SL7 1TB in relation to data transfers, maintenance of the CCR , data quality, data integration, development and enhancements;

14.4.2 Graphnet Health Limited, Station House, Station Road, Newport Pagnell, MK16 0AG, or successor bodies, in relation to data transfers, maintenance of the CCR systems, data quality, data integration, development and enhancements.

14.4.3 Countess of Chester Hospital NHS Foundation Trust, Countess of Chester Health Park, Liverpool Road, Chester. CH2 1UL in relation to the extraction of data from Cheshire Care Record CareCentric Systems.

15 CCR Information Governance Committee

15.1 There will be a CCR Information Governance Committee for this DPA. The terms of reference for the CCR Information Governance Committee will be agreed by and periodically reviewed by the signatories.

15.2 The purpose of the CCR Information Governance Committee is to make collective decisions as joint data controllers of the data shared and processed under this DPA, to the extent that the data is personal data, and to exercise control of the Processor, including overseeing, supporting and maintaining the secure sharing of data under this DPA, and to receive and review reports concerning the operations of the Processor:

15.2.1 The performance of this DPA;

15.2.2 Complaints received about the DPA;

15.2.3 The Processor's risk register and any Data Protection Impact Assessments relating to processing carried out under this DPA;

15.2.4 Due diligence on proposed new sub-contractors;

15.2.5 compliance of sub-processors with the obligations set out in this DPA; and

15.2.6 security reporting and incident reporting.

15.3 The CCR Information Governance Committee may regulate its own procedures subject to the provisions of this DPA.

15.4 CCR Information Governance Committee shall make recommendations to members of any substantial change to this DPA, and decisions will be adopted by majority decision.

15.5 CCR Information Governance Committee may make operational decisions by consensus of the majority of Signatories attending a CCR Information Governance Committee meeting as long as quorate numbers of Signatories representatives are in attendance. Before any CCR Information Governance Committee decision are taken, those taking the decision shall satisfy themselves that they are authorised to do so by those they represent.

15.6 The CCR Information Governance Committee shall have the following powers and responsibilities:

15.6.1 to approve additional Signatories joining this DPA;

15.6.2 to determine whether a Signatory shall cease to be a party to this DPA for a specific period of time or permanently for non-compliance;

15.6.3 to determine whether a Signatory may derogate from or amend any requirement under this DPA;

15.6.4 to monitor and approve the ways in which information is used pursuant to the Purposes set out in this DPA;

15.6.5 to maintain an information conduit between the Signatories;

15.6.6 to investigate (or commission the investigation of) breaches of the DPA and require Signatories to take remedial actions;

15.6.7 to monitor each Signatory's compliance with this DPA. The CCR Information Governance Committee may request evidence of compliance with this DPA on written request to any Signatory;

15.6.8 to approve any proposed amendment to the information sharing arrangements (including for the avoidance of doubt any major system upgrades or changes that could impact the security of the system);

15.6.9 to approve common patient and public communication materials and take a proactive role in ensuring effective communication about information sharing under this DPA;

15.6.10 to develop, review and maintain the DPA to ensure that it reflects any legal and statutory obligations and any other related best practice guidance in relation to information governance; and

15.6.11 to approve the information governance arrangements relating to the appointment of any processor or sub-processor by any Provider Signatory or third party to ensure that they comply with the principles of Part B.

15.7 The CCR Information Governance Committee may approve the following things provided that the groups terms of reference are met:

15.7.1 the use of data under Part A of this DPA for other purposes related to the purposes of this DPA;

15.7.2 amendments to this DPA (including its extension);

15.7.3 the appointment of any new Sub-contractor or sub-processor;

15.7.4 the appointment of any processor or sub-processor.

15.8 The following process must be followed for approving any of the things:

15.8.1 all Signatories must be made aware of the proposal (at IG lead / Caldicott Guardian / SIRO level) and given reasonable opportunity to consider, comment upon and object to the proposal. The period for consideration will be two weeks unless the CCR Information Governance Committee decides that it is reasonable to set a longer or shorter period;

15.8.2 the CCR Information Governance Committee must consider any comments and/or objections received:

(a) if the CCR Information Governance Committee is satisfied that the action proposed is lawful and will not materially increase the risk of a breach of the Data Protection Legislation arising from the arrangements provided for in this DPA, the CCR Information Governance Committee may approve the proposal and it may be implemented immediately; or

(b) the CCR Information Governance Committee may decide to re-circulate the same or a revised proposal to all Signatories in accordance with clause 15.11.1 within the DSP, then re-consider the proposal in accordance with this clause 15.11.1 within the DSP.

15.9 Any Signatory that does not agree with an action approved by the CCR Information Governance Committee pursuant to clause 15.11.2(a) within the DSP, may within 20 working days of the CCR Information Governance Committee notifying Signatories of the decision, terminate its participation in this DPA immediately by giving written notice to the CCR Information Governance Committee, without any consequent liability to the continuing Signatories.

15.10 Notice given pursuant to clause 15.14 shall be deemed served on the CCR Information Governance Committee provided such notice is delivered to the address of the Signatory whose representative is then Chair of the CCR Information Governance Committee, addressed to the Chair.

15.11 Each Signatory confirms that its Caldicott Guardian or SIRO has reviewed and agrees with the provisions of this DPA.

16 Confidentiality

16.1 The Processor agrees to keep secret and strictly confidential any Confidential and Personal Data it may receive directly or indirectly from the Controller and undertakes not to disclose any such information without written permission from the Controller unless disclosure is required by law.

16.2 The Processor agrees not to use Confidential information for any purpose other than the purpose for which it was disclosed to the Processor by the Controller.

16.3 The Processor shall ensure that all such information is treated as confidential by its employees, agents and sub-contractors.

16.4 The Processor shall ensure that all such information is treated as confidential by its employees, agents and sub-contractors.

16.5 The undertakings in clauses 3.1, 3.2 and 3.3 will continue in force indefinitely.

17 Freedom of Information and transparency

17.1 The Processor recognises that public authorities are subject to the requirements of the Freedom of Information Act 2000 (FOIA) and the Environmental Information Regulations (EIR). Any such requests relating to information governed by this DPA should be directed promptly to the Controller.

17.2 The Processor agrees to assist and co-operate with the Controller in order that it may carry out its obligations under FOIA, EIR and any transparency requirements under the UK Government Transparency Agenda. The final decision about disclosure of information or application of exemptions shall rest solely with the Controller.

18 Nomination of contacts

18.1 Each party to the DPA will identify a nominated contact point. Contact details of the nominated contact will be maintained in the CCR Governance Contact Information Document. Where the employment of a Data Protection Officer (DPO) is a legal requirement, this should be the DPO.

18.2 Where nominated contact points changes this must be updated as soon as possible.

19 Liabilities and indemnities

19.1 The Processor agrees to indemnify the Controller against any loss, damages, expenses, cost, claims, penalties or proceedings arising from the Processor's unlawful or unauthorised processing, loss, destruction and/or damage to the Controller's Personal Data and any breach of this DPA for which the Processor or its sub-processors may be liable.

19.2 Each Party shall accept responsibility for its own acts and omissions.

19.3 Nothing in this DPA shall limit liability for death or personal injury resulting from negligence or for fraud.

19.4 The Processor's liability, in its capacity as such, shall be governed by the remainder of this clause 19.

19.4.1 The Processor shall use reasonable endeavours to ensure that each of its Sub-contractors under this DPA accepts liability to the Processor for any loss that may be incurred by any Signatory as a consequence of any act or omission of that subcontractor.

19.4.2 If a Provider Signatory who is a data controller incurs a cost caused by that data controller breaching the Data Protection Legislation, as a result of the Processor (or its Sub-contractors) breaching the Processor's obligations as a data processor set out in this DPA, then the Processor's liability shall be limited to £500,000 of that cost.

19.4.3 Subject to clause 19.4.2, where the Processor is entitled to recover an amount in excess of the Relevant Amount from any subcontractor or subcontractors in respect of any claim under this DPA, then the Processor's liability in respect of that claim shall be limited to the amount that the Processor is entitled to recover from such subcontractor or subcontractors.

19.4.4 Subject to clause 19.4.2, where the Processor is not entitled to recover an amount in excess of the Relevant Amount from any subcontractor or subcontractors in respect of a claim (other than those covered in clause 19.4.2) under this DPA, then the Processor's liability in respect of that claim shall be limited to the Relevant Amount.

19.4.5 The Relevant Amount shall be £100,000.

19.4.6 Each Partner Organisation warrants that in accessing the CCR it shall comply with the licence terms set out in Schedules 2 – 16 of the Software Contract (the form of which is attached as Appendix A). Each Partner Organisation shall indemnify and keep indemnified CoCH (in its capacity as Host) from and against all costs, claims, demands, liabilities, expenses, damages or losses (including without limitation consequential losses and loss of profit, and all interest, penalties and other legal and other professional costs and expenses) arising out of or in connection with:

19.4.6.1 The use of shared data by the Partner Organisation

19.4.6.2 Personal injury caused by or arising from the Partner Organisation's use of shared data

19.4.6.3 The Partner Organisation's failure to comply with the licence terms in Schedule 2 – 16 of the Software Contract or:

19.4.6.4 The Partner Organisation's failure to comply with all applicable laws and regulations with respect to the shared data or the infringement of the rights of any third party arising out of the possession, processing or use of the shared data.

20 Variation

20.1 No variation of this DPA shall be effective unless:

20.1.1 it is in writing and signed by each of the parties; or

20.1.2 it has been approved by the CCR Information Governance Committee.

21 Term and termination

21.1 This DPA shall commence on the Commencement Date and shall continue until 14th May 2021 unless terminated earlier, or unless the CCR Information Governance Committee resolves to extend it to a further specified date.

21.2 Save where terminating in accordance with clause 15.14 of this DPA (CCR Information Governance Committee), a Signatory, which is considering terminating its participation in this DPA, shall notify the CCR Information Governance Committee of its intention and reasons, and agrees to liaise with the CCR Information Governance Committee for at least two (2) weeks, before giving notice of termination, to ascertain whether its concerns can be addressed. Having done so, a Signatory may terminate its participation in this DPA by giving three (3) months' written notice.

21.3 The CCR Information Governance Committee may decide to terminate this DPA.

21.4 Upon exiting this DPA (whether by leaving, or because the DPA has terminated or expired):

21.4.1 An exiting Signatory shall cease accessing any Individual Integrated Care Record and/or Case Finding Information immediately and securely return or destroy any shared information in its possession;

21.4.2 The Processor shall arrange for the cessation of the exiting Signatory's access to the Software; and

21.4.3 The Processor shall ensure that PCD for which the exiting Signatory is data controller is removed from the CCR Integrated Care Record at the next extract following the Signatory's exit.

21.5 Any former Signatory shall have access to audit trails only on the written authority of the CCR Information Governance Committee or as required by law.

21.6 The termination of this DPA, for whatever reason, shall not affect the accrued rights or obligations of either Party arising out of this DPA.

22 Third parties

22.1 A person who is not a party to this DPA shall not have any rights under or in connection with it (whether under the Contracts (Rights of Third Parties) Act 1999 or otherwise).

23 Notices

23.1 All notices that are required to be given under this DPA shall be in writing and shall be sent to the address of the Signatory set out in the relevant executed Signature Page.

24 Invalidity

24.1 In the event that any provision of this DPA is determined by any court of competent jurisdiction to be invalid, unlawful or unenforceable to any extent, such provision shall, to that extent, be severed from the remainder of this DPA, which shall continue to be valid to the fullest extent permitted by law.

25 Entire agreement

25.1 This DPA and its appendices constitutes the entire agreement relating to its subject matter and supersedes all previous verbal or written proposals and agreements between the Signatories.

26 Counterparts

26.1 This DPA may be executed in any number of counterparts, each of which shall be regarded as an original, but all of which together shall constitute one agreement binding on all of the parties, notwithstanding that all of the parties are not signatories to the same counterpart.

26.2 This DPA shall not be effective until the Processor and at least one other signatory has executed a counterpart.

26.3 Any Signatory, which executes a counterpart after the Commencement Date, shall be bound by the terms of this DPA from the date of that Signatory's signature.

27 Status, governing law and jurisdiction

27.1 To the extent that this DPA governs arrangements between data controller(s) on the one hand and data processor(s) on the other hand, it shall be governed by the laws of England and Wales, and the English courts shall have exclusive jurisdiction to settle any dispute or claim that arises out of or in connection with it or its subject matter or formation.

27.2 Where necessary, this Data Processing Agreement is also an NHS Contract between NHS bodies, as defined by the NHS Act 2006.

28 Signatories

28.1 By signing this DPA, all signatories accept responsibility for its execution and agree to ensure that staff are trained so that requests for information and the process of sharing itself are sufficient to meet the purpose of this DPA.

28.2 By signing this DPA the Processor certifies that:

28.2.1 the Processor meets the registration requirements of the Digital Economy Act 2017 and that this is maintained for the life of the DPA, and

28.2.2 is legally entitled to undertake the Processing agreed in this DPA

28.3 Each Signatory confirms that its Caldicott Guardian or SIRO has reviewed and agrees with the provisions of this DPA.

3 Schedule 1: Glossary and definition of terms

1. In this DPA unless the context otherwise requires the following words and expressions shall have the following meanings:

Contract	means any contract associated with this DPA, including NHS standard terms and conditions for the supply of goods and provision of services.
Data Processing Agreement or DPA	means this data processing agreement
Data Protection Legislation	means the Data Protection Act 2018, the EU Data Protection Regulation 2016/679 and all applicable laws and regulations relating to processing of personal data and privacy, including where applicable the guidance and codes of practice issued by the Information Commissioner or any NHS regulatory or advisory body, including but not limited to the Caldicott Reports relating to the sharing and processing of patient data;
Personal Confidential Data	means personal information about identified or identifiable individuals, which should be kept private or secret. For the purposes of this DPA 'personal' includes the definition of 'Personal Data', but it is adapted to include dead as well as living people. 'Confidential' includes both information 'given in confidence' and 'that which is owed a duty of confidence' and is adapted to include 'Special Categories Data' as defined in this DPA;
Processing	shall have the same meaning as set out in the GDPR as amended by the UK Data Protection Act 2018
Protective Measures	means appropriate technical and organisational measures which may include: pseudonymising and encrypting Personal Data, ensuring confidentiality, integrity, availability and resilience of systems and services, ensuring that availability of and access to Personal Data can be restored in a timely manner after an incident, and regularly assessing and evaluating the effectiveness of such measures adopted by it.
Provider Signatories	means all the signatories to this DPA who provide health or social care
Signatories	means the organisations party to this DPA.

Sub-processor	means any third party appointed to Process Personal Data on behalf of the Processor related to this Contract.
Integrated Care Record or CCR Record	means the shared electronic integrated care record collating coded patient information stored in a centralised data warehouse maintained by the Processor related to the delivery of health or social care of patients of Provider Signatories and to which Provider Signatories will have access in accordance with the provisions of this agreement.
CCR De-identified Dataset	means data that has been de-identified to ISB1523: Anonymisation Standard for Publishing Health and Social Care Data and successor standards accepted by SCCI for publication under the Health and Social Care Act 2012.

4 Schedule 2: Data inclusions and exclusions

Revision History:

Version Date Summary of Changes

The data held in the CCR Integrated Care Record are supplied as data feeds from various local systems at each organisation providing data. Each feed is translated into one or more viewing screens on the Software portal.

The process for data feeds is as follows:

- The Signatory decides what information should be contributed to the record
- The technical teams of the Provider and the Processor / Sub-contractor agree on a detailed specification for each feed
- The Signatory organises or develops the information feed
- the Sub-contractor deploys the receiver for the message and a viewing screen for the data items
- Once this technical work has been completed, the specification, the operation of the feed (method and timing) and screen shots of the data to be displayed are combined into a data feed definition document which is used for:

o sign-off by the Signatory to ensure that the information available to view conforms with the agreement to share

o acceptance testing to ensure that the data is imported correctly and the feed is otherwise fit for purpose.]

Each Signatory will share the information specified in the following data templates. The agreed exclusion codes are also set out below.

Data templates and Exclusion codes

The data templates are set out in a separate document, entitled CCR Information Sharing and Processing Agreement: Data templates. This document may not be amended without Governing Group approval.

Exclusion Codes can be located in the attached document:

Exclusion Codes.docx

5 Schedule 3: Data security and governance

1. This schedule comprises data handling standards which must be met by the Processor and imposed by the Processor through contract on approved Sub-Processors.
2. The Processor is accountable for ensuring that Sub-Processors are capable of meeting the required standards before entering in to a contract with that Sub-Processor
3. The Processor is responsible for on-going monitoring on the compliance with these terms by the Sub-Processor and any approved onward sub-processing and reporting to the Governance Committee on compliance and at frequencies determined by the CCR Information Governance Committee
4. The CCR Information Governance Committee may request auditing and testing of compliance against contracted requirements as they may reasonably require for their assurance of compliance with these contract terms
5. The Processor must impose on sub-processors a legally binding contract that:

    a. defines the status and relationship of the parties as processor and sub-processor;
    b. Identifies who the controllers are;
    c. includes a requirement to keep all personal information confidential during the term of the contract and survives contract termination;
    d. defines when data may be disclosed because it is required by law;
    e. defines what measures must be operated to protect de-identified data from re-identification;
    f. includes protection of the confidentiality of commercially sensitive information;
    g. lists people authorised to make changes and the change process;
    h. Includes a duty to co-operate with other parties;
    i. requires rapid reporting of requests for information which may fall under the Freedom of Information Act 2000 and Environment Information Regulations 2004 and which may apply to the ultimate controllers or the Processor;
    j. requires the inclusion of the contact details of significant persons for day to day management of the service or provision;
    k. defines a dispute resolution process;
    l. protects Controllers from charges, costs and liabilities, and provides indemnity, remedies and penalties for any breach or failure by the sub-processor in which the sub-processor is negligent;
    m. includes a signature page appropriate to the contract form – simple or deed;
    n. Defines what actions are required if the sub-processor is taken over, goes out of business or is in administration;
    o. there is adherence to legal and professional standards by sub-processor staff, in particular in relation to data protection, human rights and common law obligations;
    p. defines that the law under which the contract operates is English

q. lists the name and contact details of all pertinent data protection officers, for each organisation involved in the processing. There must be a mechanism included for updating or changing the DPO name and details;

r. provide that the processor must only act on direct instruction of the controller;

s. limits processing to only that permitted in contract without further written instruction;

t. Defines what happens to the data at termination (destroy and/or return) including standards of destruction and what evidence must be provided of destruction and how data would be returned;

u. requires that permission to audit cannot be reasonably withheld, and for assurance through shared audit (dependent on the risks of processing);

v. imposes performance and security test reporting and report frequency;

w. restricts onward sub-processing without prior written approval first being obtained;

x. the processor is held to provide sufficient guarantees that they can implement appropriate technical and organisational measures that will meet the requirement of the regulation;

y. that sub-processor's employees and others with access to the data have an appropriate contract of employment which holds them to keep any information they access confidential and to only act on the written instructions of the controller;

z. the processor will operate all necessary security measures to protect the data from malicious attack, loss or destruction and that they will be regularly tested for resilience;

aa. includes (GDPR §31), a contract must specify that Business Continuity and Disaster recovery processes are in place and will be monitored.

bb. includes (GDPR §32(1)) evidence required to substantiate security of processing;

cc. includes, related to GDPR §33 that all breaches relating to the data are reported within a specific timescale (recommended 12 hours) and that records are kept specifically where they relate to the data processed by the data processor. It must also restrict the processor to only reporting details of the breach to the controller and to no other entity unless required to by the supervisory authority. This allows the data controller time to comply with the requirement to report to the supervising authority within 72 hours any major data breach.

dd. The regulation at §33(2) stipulates without delay.

ee. a mechanism for breach reporting must be included either in the schedules or the contract itself and must be specific about the data affected;

ff. Data Protection Impact Assessment and risk management;

gg. GDPR §35, the contract should include the requirement to take part in and assist with DPIAs. This is a requirement on the controller in respect of the regulation. However, the volume and nature of processing may make it reasonable to have a clause which describes how the processor will

assist in this process including if a Data Protection Impact Assessment been carried out for the sub-contracted services;

hh. include the requirement to create and maintain an up-to-date risk register for the processing;

ii. records of Processing Activities;

jj. stipulate what records are to be kept of the processing activities undertaken and that the processor will provide a copy on demand This must include:

kk. (a) the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;

ll. (b) the categories of processing carried out on behalf of each controller;

mm. (c) 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 §49(1), the documentation of suitable safeguards;

nn. (d) where possible, a general description of the technical and organisational security measures referred to in Article 32(1);

oo. maintenance of information asset registers - Caldicott (2013);

pp. schedules must be structured in such a way that each flow of data is appropriately stated, and the lawful basis for each is clearly described along with those that are allowed to process the data. Each flow may involve different controllers, processors and sub-processors. The schedules should include the following:

qq. a description of the categories and types of data to be processed including an embedded agreed dataset if required;

rr. the purpose of the processing, including the lawful basis (Caldicott (2013) Appendix 6(7);

ss. the data controllers involved (if multiple) and who is able to give instruction - note this may be different if different flows have different Data Controllers;

tt. the Data Processors who are allowed to process the data;

uu. the recipients of each flow of data and the processing allowed (may be similar to the above);

vv. categories of data subject;

ww. the arrangements and responsibilities to respond to subject access requests, the right to erasure and data portability;

xx. the arrangements and responsibilities for fair processing information, including service user involvement in its development (Caldicott (2013));

yy. if the data is transformed or changed in any way through the flow to another organisation;

zz. security expectations around the transfer of the data and the data at each state of rest;

aaa. access controls to be applied to the data (who can have access at each element of processing);

bbb. the retention period of the data (including after the contract is terminated) and in what form it should be returned to the owner;

ccc. the allowed geographical location of the data and any controls or restrictions;

ddd. security testing and assurance regime for the processing (where required);

eee. either a restriction on access from, transfer to a third country, or authority to transfer dependent on;

fff. general principles for transfers;

ggg. transfers on the basis of adequacy decisions, where relevant;

hhh. transfer subject to appropriate safeguards, where relevant;

iii. binding corporate rules, where relevant;

jjj. policies and procedures on consent;

kkk. conflicts of interest management and evidence;

lll. data extraction processes;

mmm. details of security requirements, e.g. access controls, secure transfers, device security including encryption, etc. with suitable evidence.

6 Schedule 4: Processor service charges

These will be charged at current market value and will be inclusive of VAT. Whilst estimates of charges will be given it should be noted that actual costs can change without liability to CoCH.

7 Schedule 5: Data Protection Impact Assessment

DPIA Report - Cheshire Care Recor

8 Schedule 6: Sharing Agreement

CCR Information Sharing Agreement.

9 Schedule 7: Signatories List

- Cheshire East Borough Council
- Cheshire West & Chester Council
- 18 GP Practices in South Cheshire CCG
- 12 GP Practices in Vale Royal CCG
- 23 GP Practices in Eastern Cheshire CCG
- 37 GP Practices in West Cheshire CCG
- Mid Cheshire Hospitals NHS FT (MCHFT)
- East Cheshire NHS Trust (ECNT)
- The Christie NHS FT
- Cheshire and Wirral Partnership NHS FT (CWP)
- East Cheshire Community NHS Trust
- Countess of Chester NHS FT (CoCH)
- Clatterbridge Cancer Centre NHS Trust.

1.1.1 Name	1.1.2 Initials	1.1.3 Organisation	1.1.4 Attendance
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	

[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	
[redacted]	[redacted]	[redacted]	

10 Schedule: 8 Signatories Page

IN WITNESS WHEREOF the Parties have caused this agreement to be executed as a deed on 14th May 2019

This Agreement should only be signed by the Parties Caldicott / Deputy Caldicott Guardian, Senior Information Risk Owner (SIRO), Chief Executive or another Board Level / Appropriate Senior Manager.

EXECUTED AS A DEED by

Organisation:	Countess of Chester Hospital NHS Foundation Trust
Name:	[redacted]
Position:	Caldicott Guardian
Signed:	[redacted]
Date:	15 May 2019

EXECUTED AS A DEED by (please complete all fields)

Organisation:	
Name:	
Position:	
Signed:	
Date:	